KU LEUVEN

CENTRE FOR IT & IP LAW

Faculty of Law

REGULATING DATA PROTECTION

THE ALLOCATION OF RESPONSIBILITY AND RISK AMONG ACTORS INVOLVED IN PERSONAL DATA PROCESSING

Brendan VAN ALSENOY

Supervisor:
Prof. P. Valcke

Co-supervisor:
Dr. E. Kindt

Jury members:

Prof. G. Van Overwalle
Prof. S. Gutwirth
Prof. G. Sartor

Thesis submitted with a view
to obtaining the degree of
Doctor of Laws

Academic year 2015-2016

August 2016

Acknowledgments

Early in my academic carreer, a learned professor told me: “the only good PhD is a finished PhD”. What he didn’t tell me, at the time, was that it takes a village to actually finish it. Completing this thesis would not have been possible without the support of my colleagues, family and friends.

I would like to begin by thanking my supervisor, Prof. Dr. Peggy Valcke, for her guidance, encouragement and trust. She gave me time and space to develop my own research, yet was there to provide practical direction whenever needed. Warm thanks are also due to my co-supervisor, Dr. Els Kindt, for her insightful comments and continuous support. I am indebted to the members of my advisory committee, Prof. Dr. Geertrui Van Overwalle and Prof. Dr. Serge Gutwirth, for their invaluable feedback and the references they provided. I thank Prof. Dr. Giovanni Sartor not only for acting as a member of my examination committee, but also for the fresh and critical perspective one so often encounters in his writing. My gratitude goes out to Em. Prof. Dr. Marc Boes for kindly agreeing to chair the examination committee. Finally, I would like to thank Em. Prof. Dr. Jos Dumortier for his advice and support at the beginning of my PhD project.

Working at the Centre for IT & IP law (CiTiP) has been an honour and a privilege. It is an environment filled with bright minds, dedicated people and a passion for knowledge. I would like to thank every one of my colleagues - past and current - for all the stimulating conversations, comradery and fond memories. Special thanks go out to Fanny Coudert, Jef Ausloos, Bjorn Coene and Yung Shin Van der Sype for providing me with ideas and feedback throughout the writing process. I would also like to thank Kirsten Van Gossum, Griet Verhenneman, Niels Vandezande, Aleksandra Kuczerawy, Eva Lievens, Eleni Kosta, Valerie Verdoodt, Jessica Schroers, Lina Jasmontaite and Ellen Wauters for the great collaboration in the many projects along the way. Finally, I would like to express my sincere appreciation to Shuki Tang, Carmen Clara, Edith Appelmans and Linda Mees, for their unique combination of professionalism and warmth when supporting our research activities on a daily basis.

The findings in this thesis have benefited from the input of many people outside my university department. I would especially like to thank Prof. Dr. Spiros Simitis and the Hon Michael Kirby for sharing valuable insights in relation to the 1970 Hesse Data Protection Act and the 1980 OECD Privacy Guidelines. I am extremely grateful to Michael Donohue for giving me the opportunity to join the OECD Secretariat during the revision of the OECD Privacy Guidelines, as well as for his comments on my research. Dr. Lina Kestemont provided me with invaluable support on how to navigate issues of legal methodology, without which my hermitage perhaps would have been prolonged indefinitely. I thank Joseph Alhadeff for introducing me to the world of multi-

stakeholder policy development and for our many lively discussions. I thank Danny De Cock, Günes Açar, Claudia Diaz and Seda Gürses for showing me how cool working with computer scientists can be. Finally, I would like to thank Joelle Jouret for reviewing and commenting on the sections concerning the General Data Protection Regulation.

Last but not least, I would like to thank my family, friends and loved ones. I thank my parents for their unwavering encouragement and support, both in research and in life. I thank my sister for being such an inspiration. I thank Dieter for keeping me grounded and for teaching me that long sentences do not make you seem smarter. I thank Paula for keeping me well nourished and hydrated during the final stages of the writing process. Finally, I thank Aleksandra for her patience, indulgence and caring, and for giving me the motivation to keep going on.

Brendan Van Alsenoy

July 2016

Abstract

Practically every organisation in the world processes personal data. In fact, it is difficult to imagine a single organisation which does not regularly collect, store or access information about individuals. European data protection law imposes a series of requirements designed to protect individuals against the risks that result from the processing of their data. It also distinguishes among different types of actors involved in the processing and sets out different obligations for each type of actor. The most important distinction in this regard is the distinction between "controllers" and "processors". Together, these concepts provide the very basis upon which responsibility for compliance with EU data protection law is allocated. Unfortunately, technological and societal developments have rendered it increasingly difficult to apply these concepts in practice. The complexity of today's processing operations is such that a clear-cut distinction between "controllers" and "processors" is not always possible. Identifying "who's who" can be particularly difficult when the processing involves a large number of actors, who each play their own distinct role in realising the goal(s) of the processing.

Against this background, this thesis seeks to determine whether EU data protection law should maintain its current distinction between controllers and processors as the basis for allocating responsibility and risk. Specifically, it seeks to determine whether it would be possible to modify the current approach in a manner which would increase legal certainty, without diminishing the legal protections enjoyed by data subjects. To realise these objectives, this thesis undertakes an analysis consisting of four parts. It begins by detailing the nature and role of the controller and processor concepts under current data protection law (Directive 95/46). Next, an historical-comparitive analysis traces the origin and development of the controller-processor model over time. After that, a number of real-life use cases are examined, with the aim of documenting the issues that arise when applying the controller-processor model in practice. Once the issues have been analysed, an evaluation is made of potential solutions. Finally, the approach adopted by the European legislature in the context of the General Data Protection Regulation (GDPR) is compared with the outcome of the preceding evaluation.

The thesis concludes that while the GDPR introduces considerable improvements, a number of recommendations can still be made. First, the possibility of abolishing the distinction between controllers and processors should receive further consideration. It is possible to implement the same policy choices without retaining these problematic concepts. Alternatively, the definitions of each concept could be revised to include less ambiguous as well as mutually exclusive criteria. Second, the legislature should consider the use of standards (as opposed to rules) to mitigate certain risks of overinclusion. Third, the obligation to implement data protection by design should eventually also be made directly applicable to the providers of processing services, given their important role in determining the means of the processing. Fourth, the legal framework should

allow for contractual flexibility in the relationship between "controllers" and "processors", leaving room for greater specificity in the form of regulatory guidance. Finally, the scope of the personal use exemption should be expanded to apply to all activities which may reasonably be construed as taking place in the course of an individual's private or family life.

TABLE OF CONTENTS

PART I

INTRODUCTION

Chapter 1 BACKGROUND

1. THE ORIGINS OF DATA PROTECTION LAW – Automated processing of personal information has always been a topic of controversy. As soon as computers became visible to the general public, reflections on how computers might impact the privacy of individuals began to enter the political arena.[1] The first data protection laws emerged during the 1970s, with the aim of protecting individuals against risks resulting from the automated processing of personal data.[2] Regulatory initiatives at the international level soon followed. The first international organisation to formally adopt a normative stance in relation to the processing of personal data was the Council of Europe in 1973.[3] In 1980, the OECD adopted its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[4] In 1981, the Council of Europe promulgated the *Convention for the protection of individuals with regard to automatic processing of personal data* (Convention 108).[5]

2. INITIATIVES AT EU LEVEL – Even after Convention 108 came into effect, notable differences in national data protection laws remained. As the European Union developed, these differences were perceived as potential obstacles towards the development of the Internal Market.[6] In 1990, the European Commission put forth a draft for a Council Directive on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data. This proposal eventually led to the adoption of *Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data*.[7] In 2016, the *Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) was adopted.[8] This Regulation is set to repeal and replace Directive 95/46 as of 25 May 2018.

---

[1] See C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992, 2.

[2] P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen/Oxford, Intersentia, 2006, p. 76. See also R. Gellert, "Understanding data protection as risk regulation", *Journal of Internet Law* 2015, p. 3-16.

[3] Committee of Ministers of Council of Europe, Resolution (73)22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973 (224th meeting of the Ministers' Deputies).

[4] Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980.

[5] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981.

[6] F.H. Cate, "The EU Data Protection Directive, Information Privacy, and the Public Interest", *Iowa Law Review* 1995, Vol. 80, p. 432.

[7] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, *O.J.* 23 November 1995, L 281/31. Hereafter also referred to as "Directive 95/46/EC" or simply "the Directive".

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

3. THE IMPORTANCE OF ROLES AND RESPONSIBILITIES – As with any legal instrument, it is essential to establish not only the substantive provisions of regulation, but also to identify which actors shall be responsible for ensuring compliance. Data protection law is no different in this regard. As Hondius observed:

> *"for an effective system of data protection it is of great importance that the role, rights, and responsibilities of the various persons and parties involved be stated unambiguously*".[9]

4. RELEVANT ACTORS – Under EU data protection law, there are at least two actors implicated by the processing of personal data: a "controller" and a "data subject". A data subject is essentially any individual to whom the data relates, provided that he or she is identified or sufficiently identifiable.[10] The controller is defined as the party who alone, or jointly with others, "determines the purposes and means" of the processing.[11] A third important actor identified by EU data protection law is the "processor". A "processor" is defined as a party who processes personal data on behalf of the data controller.[12] Both the controller and the processor concepts are essential to the regulatory scheme of European data protection law. Together, these concepts provide the very basis upon which responsibility for compliance is allocated.

5. ALLOCATION OF RESPONSIBILITY AND RISK – Under Directive 95/46, the allocation of responsibility and risk among controllers and processors results from a combination of provisions. As far as the controller's obligations are concerned, the allocation of responsibility is in first instance the result of article 6(2) of the Directive. This provision stipulates that it shall be the controller who must ensure that the basic principles of data protection are complied with. In addition, the Directive specifies a wide range of additional obligations (e.g., accommodation of data subject rights, maintaining an appropriate level of security, etc.) which shall be incumbent upon the controller. Finally, article 23 of the Directive explicitly confirms that the liability for damages caused by non-compliant behaviour shall be borne by the controller, unless he is able to avail himself of an exemption. As far as the processor's obligations are concerned, the Directive is far more succinct. In fact, it articulates obligations addressed

---

such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* 4 May 2016, L 119/1. Hereafter referred to as the "General Data Protection Regulation" or "GDPR".

[9] F. W. Hondius, *Emerging data protection in Europe*, North-Holland Publishing Company, Amsterdam, 1975, p. 101.

[10] See article 2(a) Directive 95/46 and article 4(1) GDPR. See also B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *Identity in the information society* 2009, Vol. 2, n°1, p. 68 (available at http://www.springerlink.com/content/u11161037506t68n/fulltext.pdf, last accessed 24 November 2010). For a more detailed discussion see Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", WP 136, 20 June 2007, 26 p., available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (last accessed 11 May 2016).

[11] Article 2(d) Directive 95/46; article 4(7) GDPR.

[12] Article 2(e) Directive 95/46; article 4(8) GDPR.

directly towards the processor in only one instance.[13] Under the GDPR, the allocation of responsibility and risk among controllers and processors has been modified considerably. While the controller is still the party who carries primary responsibility for compliance with data protection principles (article 5(2)), processors have become subject to a host of obligations and may be directly liable towards data subjects in case of an infringement (article 82).

6. ADDITIONAL FUNCTIONS – Both the controller and processor concepts are relevant for a range of other legal questions, such as which law applies to the processing.[14] Both concepts are thus pivotal in determining the scope of European data protection legislation, not only by reason of the type of actor concerned (*ratione personae*), but also as concerns the applicability of national provisions (*ratione territoriae*). As a result, the interpretation of these concepts shall be determinative for every actor's perception of how the relevant legislation affects him or her, and what measures he or she is expected to put in place.[15]

[13] See Alhadeff, J. and Van Alsenoy, B. (eds.), "Requirements: Privacy, governance and contractual options", *Trusted Architecture for Securely Shared Services* (TAS^3), Deliverable 6.1, v2.0, 2009, p. 31 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *Computer, Law & Security Review* 2007, Vol. 23, n° 5, p. 418. See in particular art. 16 and 17 of the Directive.

[14] See Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'", WP169, 16 February 2010, p. 5, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (last accessed 14 April 2016).

[15] D. Bainbridge, *EC Data Protection Directive*, London, Butterworths, 1996, p. 116.

Chapter 2 PROBLEM STATEMENT

7. OUTLINE – Given the fundamental importance of both the controller and processor concepts, it is essential to be able to determine which role an actor has assumed towards a particular processing operation. Unfortunately, it can be quite difficult to apply the distinction between controller and processors in practice.[16] Over time, data protection authorities and courts have provided guidance to inform the practical application of the controller and processor concepts.[17] Notwithstanding the guidance, however, certain scholars have continued to question the utility of the controller-processor model.[18] The following sections outline three vulnerabilities of the current framework.

1 A BROKEN "BINARY"

8. OVERSIMPLIFICATION? – Perhaps the most common critique of the controller-processor model is that the "binary" distinction between controllers and processors is too simplistic.[19] While the model may be readily applied in certain situations, the complexity of today's processing operations is such that a clear-cut distinction between controllers and processors is seldom possible.[20] As a result, the binary distinction is

---

[16] C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, second edition, New York, Oxford University Press, 2007, 71-72. For example, portable devices have evolved from single-function apparati to complex and powerful processing systems that have the ability to support a variety of applications (e.g., voice communication, email, social networking, location-based services).

[17] See e.g. the Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596; Judgement in *Google Spain*, C-131/12, EU:C:2014:317, Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor", WP169, 16 February 2010 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).

[18] See e.g. P. Van Eecke and M. Truyens, "Privacy and social networks", *Computer, Law & Security Review* 2010, Vol. 26, 537-539; W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary University of London, School of Law, *Legal Studies Research Paper No.* 77/2011, in particular p. 10-11 and 24; O. Tene, "Privacy: The new generations", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 26; J.M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *Revue du Droit des Technologies de l'Information* 2011, vol. 42, in particular p. 40 et seq. and P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review* 2012, vol. 28, p. 133-134.

[19] See in particular P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 537; W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 24.

[20] See in particular C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 72; P. Van Eecke, M. Truyens et al. (eds.), "The future of online privacy and data protection, EU study on the Legal analysis of a Single Market for the Information Society – New rules for a new age?, DLA Piper, November 2009, p. 32 available at http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=7022 (last accessed 14 April 2016); J.M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible ?", *l.c.*, p. 40. A prime example in this regard is identity federation. See T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 417-420. See also *infra*; nrs. 662 et seq.

considered inadequate to accommodate the increasingly collaborative manner in which businesses operate.[21] Nowadays, control relationships are more complex than the "either/or" approach of the controller-processor model; whereby one party (or group of parties) exercises complete control over the processing, and another party (or group of parties) simply executes the tasks it has been given, without exercising any substantial influence as to either the purposes or means of the processing.

9. EVOLVING PROCESSING PRACTICES – At the time Directive 95/46 was adopted, the distinction between parties who control the processing of personal data (data controllers) and those who simply process the data on behalf of someone else (data processors) was relatively clear.[22] Today we are confronted with a "growing tendency towards organisational differentiation".[23] In both the public and private sector

> *"there is a growing emphasis on the development of delivery chains or service delivery across organisations and on the use of subcontracting or outsourcing of services in order to benefit from specialisation and possible economies of scale. As a result, there is a growth in various services, offered by service providers, who do not always consider themselves responsible or accountable […]."*[24]

10. DISTRIBUTED CONTROL – To be clear, the diversification and specialization of the market for processing services does not in and of itself implicate the providers of those services as controllers or co-controllers. In addition to the expansion of the processing market, however, there is also an increase in collaboration among otherwise autonomous entities whose mutual relationships can no longer be characterized as a simple "principal-delegate" relationship. Similarly, we are also witnessing an increase in services whose use is available to many but the purposes and means of the processing have - at least in the abstract - been determined largely in advance. The assumed power of the controller may therefore in practice be "carved out", to a greater or lesser extent, by the power of (or choices made by) other parties with whom it interacts, even though the legal obligations for compliance remain with the controller.[25]

---

[21] See e.g. O. Tene, "Privacy: The new generations", *l.c.*, 26; Information Commissioner's Office, "The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union", 14 January 2011, p. 9, accessible at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf.

[22] C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 71-72.

[23] Opinion 1/2010, *l.c.*, p. 6.

[24] *Id.*

[25] P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 538 (in relation to the role of users of social networks as data controllers within social networks). While the cited authors refer to the decision-making power of individual social network users, similar considerations apply in relation to the interaction among organisations.

2 THE THRESHOLD FOR (CO-)CONTROL

11. LEGAL UNCERTAINTY – European data protection law advances several criteria to determine whether an entity is acting either as a controller or a processor towards a particular processing operation.[26] While the criteria appear conceptually sound, it often remains debatable whether an entity is either acting as a controller or as a processor towards a particular processing operation. Determining the appropriate qualification of a given actor can be particularly difficult in complex processing environments, in which many actors participate. This is for example the case for so-called "integrated" services, where the final service delivered to the end-user is the result of a complex value chain, which may involve any number of intermediary processing operations (e.g., registration, authentication, authorization, discovery, retrieval, enrichment, etc.).[27]

12. MALLEABILITY OF CURRENT CRITERIA – The more actors involved in realizing a particular output or functionality, the more likely one will encounter divergent opinions as to which actor (or actors) "control" the processing from a legal perspective.[28] An additional factor that may complicate the analysis is the fact that existing resources are frequently leveraged to deliver new functionalities, rendering it difficult to assess where the "determinative influence" of each actor (and thus the scope of its respective obligations) begins and ends. While the "purposes and means" of the processing might be determined by more than one actor, it is not always clear which level of influence is required in order to implicate an actor as a (co-)controller.[29]

3 THE IMPLICATIONS OF "GRANULAR" CONTROL

13. MORE GRANULARITY, MORE PROBLEMS? – The increased complexity of processing operations has led both doctrine and practitioners to apply a less "monolithic" conception of control (particularly in cases where clearly distinct actors are

---

[26] Cf. *infra*; nrs. 65 et seq.

[27] See also J. Alhadeff and B. Van Alsenoy (eds.), "Legal and Policy handbook for TAS^3 implementations", *Trusted Architecture for Securely Shared Services* (TAS^3), Deliverable 6.1-6.2, v1.0, 2012, p. 91-92, available at http://homes.esat.kuleuven.ac.be/~decockd/tas3/final.deliverables/pm48/TAS3-D06p1-2_Legal_and_Policy_Handbook_final_versionforthereviewers.pdf (last accessed 28 April 2016).

[28] See, for example, the report issued by the Biometrics & eGovernment Subgroup of the Working Party in relation to the STORK project (acknowledging that the subgroup was not able to come to a concordant conclusion as to whether or not a pan European proxy service ("PEPS") should be considered as a (co-)controller or processor; despite the guidance provided by the Article 29 Working Party in Opinion 1/2010. (Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, Written Report concerning the STORK Project, Ref.Ares(2011)424406, 15 April 2011, 6-7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_15_letter_artwp_atos_origin_annex_en.pdf, last accessed 1 August 2011). See also *infra*; nrs. 759 et seq.

[29] See also J. Alhadeff and B. Van Alsenoy (eds.), "Legal and Policy handbook for TAS^3 implementations", *l.c.*, p. 91 et seq.; T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 419; C. Kuner, *European data protection law: corporate compliance and regulation*, *o.c.*, p. 70.

participating in the processing of personal data).[30] Under this approach, a distinction is first made between the different types of processing operations in order to determine which role each actor plays with regards to each operation. In addition, the controller concept is applied with increased granularity, in particular by recognizing that the "degree" to which a particular actor exercises a determinative influence over the purposes and means of the processing can vary significantly.[31] This more granular and flexible approach seems to create tension with other provisions of EU data protection law, as well as some of its underlying objectives.

14. TRANSPARENCY – A first area of concern relates to the transparency of processing. Every controller is in principle under an obligation to identify himself towards the data subject.[32] One of the underlying objectives of this provision is to ensure that the data subject is aware of which actor is responsible for the processing, in order to allow him to exercise his rights as a data subject if he so chooses. In situations where a substantial number of controllers are involved, there is the risk that the data subject will not know to whom to turn in order to exercise his rights, or from whom he should seek redress in case of a privacy breach.[33] The Article 29 Data Protection Working Party has acknowledged that the multiplication of controllers may have a negative impact on the transparency of processing. Therefore, according to the Working Party

> "*the assessment of joint control should take into account on the one hand the necessity to ensure full compliance with data protection rules, and on the other hand that the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing*."[34]

15. STRATEGIC INTERPRETATIONS? – While the Working Party's motives underlying this statement appear to be well-intentioned, the cited text also makes a certain risk apparent. The risk is that the concept of a controller is interpreted differently simply because of the increased number of actors involved in the processing. The legal status of an actor as controller or processor should in principle be determined in light of its actual role in the processing, not as a result of the number of actors involved in the processing.

---

[30] See also B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 69. See also J. Alhadeff and B. Van Alsenoy (eds.), "Legal and Policy handbook for TAS[3] implementations", *l.c.*, p. 96.

[31] See Opinion 1/2010, *l.c.*, p. 19 and 22 (recognizing that "*in many cases the various controllers maybe be responsible – and thus liable - for the processing of personal data at different stages and to different degrees*."). See also B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC, *Computer Law & Security Review* 2012, Vol. 28, p. 36 et seq.

[32] See articles 10-11 of Directive 95/46/EC.

[33] See also Opinion 1/2010, *l.c.*, p. 24.

[34] *Id.*

16. ALL OR NOTHING? – A second area of tension pertains to the scope of the obligations incumbent upon controllers. The obligations incumbent on a controller in principle befall the controller "as a complete set". A controller shall in principle be accountable for every aspect of the data processing under its control: ranging from its obligation to ensure that the data quality principles are complied with, to the obligation to support the exercise of data subject rights, to notification obligations etc. In practice, the situation often occurs whereby certain obligations may more easily be fulfilled by actors other than the controller(s) himself (themselves). In Opinion 1/2010, the Article 29 Working Party emphasized that not being able to directly fulfil all the obligations of a controller does not excuse an actor from its obligations under data protection law. It may engage other actors to achieve compliance with its obligations, but this does not negate the fact that it is the controller that remains ultimately responsible for them.[35] In other opinions, however, the Working Party has adopted a seemingly contradictory approach, indicating that certain controllers might be dispensed from certain compliance obligations.[36]

[35] Opinion 1/2010, *l.c.*, 22 (stating "*It may be that in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller's behalf. However, a controller will remain in any case ultimately responsible for its obligations and liable for any breach to them.*").
[36] See e.g. Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", WP171, 22 June 2010, p. 11-12, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed 12 December 2010).

Chapter 3 RESEARCH QUESTIONS

17. MAIN RESEARCH QUESTION – The main research question of this thesis is the following:

> *Can the allocation of responsibility and risk among actors involved in the processing of personal data, as set forth by Directive 95/46 and the General Data Protection Regulation, be revised in a manner which increases legal certainty while maintaining at least an equivalent level of data protection?*

18. ALLOCATION OF RESPONSIBILITY AND RISK – In the context of this thesis, "allocation of responsibility" is understood as the process whereby the legislature, through one or more statutory provisions, imposes legal obligations upon a specific actor. "Allocation of risk", on the other hand, is understood as the process whereby the legislature, through one or more statutory provisions, imputes liability or sanctions to an actor where certain prescriptions or restrictions have not been observed.[37]

19. ACTORS INVOLVED IN THE PROCESSING – The research question is limited to actors involved in the processing of personal data. An actor may be "involved" in the processing of personal data either by processing data for themselves, on behalf of others, or by causing others to process personal data on their behalf. The research question does not extend to other stakeholders who might influence the level of data protection, such as system developers, technology designers, standardisation bodies, policymakers, etc.

20. LEGAL CERTAINTY – Legal certainty is a general principle of EU law. It expresses the fundamental premise that those subject to the law must be able to ascertain what the law is so as to be able to plan their actions accordingly.[38] One of the reasons why European data protection law introduced the distinction between controllers and processors was to clarify their respective responsibilities under data protection law, thereby increasing legal certainty.[39] Many stakeholders consider, however, that the distinction reflects an outdated paradigm, which is overly simplistic and has become increasingly difficult to apply.[40] Some even suggested that, because of its decreased

---

[37] For a comprehensive study of the concept of legal risk see T. Mahler, "Defining legal risk", paper presented at the conference "Commercial Contracting for Strategic Advantage – Potentials and Prospects", Turku University of Applied Sciences, 2007, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014364 (last accessed 15 December 2010).

[38] T. Tridimas, *The General Principles of EU Law*, 2nd edition, Oxford University Press, Oxford, 2006, p. 242 et seq.) See also J. Raitio, "The Expectation of Legal Certainty and Horizontal Effect of EU Law", in U. Bernitz, X. Groussot and F. Schulyok (eds.), *General Principles of EU Law and European Private Law*, 2013, Croyden, Kluwer Law International, Croyden, p. 199-211.

[39] See also Opinion 1/2010, *l.c.*, p. 5.

[40] See e.g. Information Commissioner's Office, "The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union", l.c., p. 9; P. De

relevance and applicability, the distinction actually creates legal uncertainty.[41] The main objective of this thesis is to explore ways in which legal certainty might be increased, without diminishing the legal protections currently enjoyed by data subjects.

21. AT LEAST EQUIVALENT – The reference, in the research question above, to "an equivalent level of data protection", refers to the protection offered by Directive 95/46/EC and the General Data Protection Regulation. Within the context of this thesis, the substantive requirements and principles of EU data protection law (e.g., finality, proportionality, transparency) are taken as a given. As a result, the research question does not directly concern the substantive principles or requirements of data protection law. Rather, it pertains to the manner in which responsibility and risk for compliance with the requirements and principles are (or should be) allocated. That being said, it remains necessary to include the principles and requirements themselves within the scope of study, if only with a view of ensuring that any proposals to revise the current allocation of responsibility and risk do not result in a lowering of the protection enjoyed by individuals (e.g., by limiting their abilities to obtain redress or by decreasing transparency of processing).

22. SUB-QUESTIONS – In developing an answer to the main research question, the following sub-questions will help guide the research:

1. What is the nature and role of the controller and processor concepts under European data protection law?
2. What is the origin of the controller-processor model and how has it evolved over time?
3. What are the types of issues that arise when applying the controller-processor model in practice?
4. Which solutions have been proposed to address the issues that arise in practice and to what extent are they capable of addressing the issues?

Each of these sub-questions corresponds with one of the main parts of this thesis.

Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 134 and European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", 2009, p. 5, available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/european_privacy_officers_forum_en.pdf (last accessed 28 April 2016).

[41] European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 5; Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", 2009, at paragraph 19, available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/bird_bird_en.pdf. See also International Pharmaceutical Privacy Consortium, "Comments in Response to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", 2009, p. 7, available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/international_pharmaceutical_privacy_consortium_en.pdf (last accessed 10 March 2016).

23. INNOVATIVE CHARACTER – Several authors have already alluded to the fact that it is becoming increasingly difficult to apply the controller and processor concepts in practice. No scholar has, however, to the best of my knowledge, undertaken a fundamental analysis of the origin and development of those concepts.[42] Moreover, the issues that undermine the controller-processor model have not yet been the subject of an in-depth study. Where issues have been identified, the observations that were made have typically been confined to the context in which they arose (e.g., social networks, cloud computing). The aim of this thesis is to go beyond these fragmented perspectives and to contribute to a more comprehensive understanding of the issues that undermine the current regulatory approach. Only by doing so, is it possible to evaluate which solutions are capable of improving the current state of affairs in a meaningful and sustainable fashion.

24. RELEVANCE – The analysis undertaken throughout this thesis is likely to benefit scholars, practitioners and policymakers who are active in the field of data protection. Specifically, it will help them to (a) better understand the nature and role of the controller and processor concepts; (b) inform them on the vulnerabilities of the current approach; and (c) outline potential ways of improving the current state of affairs.

[42] The Article 29 Data Protection Working Party has provided a partial outline of the history of these concepts in Opinion 1/2010, but this analysis did not provide an in-depth analysis of the origin and development of the controller and processor concepts. Moreover, it was limited to developments at the level of the European Union.

Chapter 4 STRUCTURE AND METHODOLOGY

25. OUTLINE – This thesis is divided into five parts, whereby each part aims to answer one of the research sub-questions identified in Chapter 3. The following sections will briefly describe the main topics that are covered by each part, as well as their methodological approaches. Further details regarding scope and methodology can be found in the introductory chapter of each part.

1 DIRECTIVE 95/46

26. RESEARCH OBJECTIVE – Part II of the thesis will analyse the nature and role of the controller and processor concepts under Directive 95/46. The aim is to obtain a better understanding of the meaning of the concepts, as well as the functions they fulfil within European data protection law. To this end, an analysis shall be made of the regulatory scheme of Directive 95/46, with special attention to (a) the definitions of the controller and processor; (b) allocation of responsibility and risk; and (c) the additional functions fulfilled by the controller and processor concepts.

27. SCOPE – The choice has been made to confine the analysis in Part II to Directive 95/46 for several reasons. First, the definitions of controller and processor contained in Directive 95/46 were incorporated by the GDPR without substantive modification. Second, most of the literature, guidance and case law interpreting the concepts of controller and processor has been developed in the context of Directive 95/46. Third, Directive 95/46 forms the backdrop against which the GDPR was developed. To properly understand the nature and role of the controller and processor concepts under the GDPR, it is necessary to first examine the meaning and role of these concepts under Directive 95/46.[43] The GDPR will be analysed, however, as part of the historical-comparative analysis conducted in Part III and when articulating policy recommendations in Part V.

28. METHODOLOGY – Part II of the thesis will follow an internal approach. The primary sources of analysis shall be the text of Directive 95/46, its preparatory works and the guidance issued by the Article 29 Working Party. Where appropriate, reference shall also be made to the preparatory works of national implementations of Directive 95/46 (e.g. the Netherlands, Belgium), as a means to clarify and supplement the insights offered by the primary sources. Finally, regard shall also be had to the Principles of European Tort Law as well as national tort law for issues not addressed explicitly by Directive 95/46.

[43] Moreover, doing so will enable a more informed evaluation of the choices made by the EU legislature in the context of the GDPR and to identify areas of further improvement. Cf. *infra*; nr. 37.

2 HISTORICAL-COMPARATIVE ANALYSIS

29. RESEARCH OBJECTIVE – Part III of the thesis will describe the origin and development of the controller and processor concepts over time. As indicated earlier, European data protection law developed only after several national and international instruments were already in place. By analysing a subset of these instruments, it is possible to further enhance the understanding of the meaning and role of the controller and processor concepts.

30. SCOPE – The historical-comparative analysis shall focus upon the development of the controller and processor concepts at national, international and supra-national level. First, three of the earliest data protection laws (i.e. of Hesse, Sweden and France) are analysed. After that, two international instruments of data protection are discussed, namely the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines") and Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ("Convention 108"). Next, two national data protection laws implementing Convention 108 are analysed, namely the UK and Belgian data protection acts, followed by a discussion of the legislative development of Directive 95/46. Finally, the General Data Protection Regulation (GDPR) and its legislative development will be analysed.

31. METHODOLOGY – The comparative analysis shall be primarily dogmatic in nature. To the extent possible, reference shall be made to primary sources (i.e. legislation, formal declarations and guidelines issued by the relevant institutions). Where appropriate, however, reference shall also be made to preparatory works and explanatory memoranda, jurisprudence, and doctrinal accounts of the meaning and implications of certain concepts.

3 USE CASES

32. RESEARCH OBJECTIVE – Part IV of the thesis aims to identify and evaluate the main issues that arise when applying the controller-processor model in practice. To this end, a number of real-life use cases will be examined, with the aim of documenting specific issues that arise when applying the concepts of controller and processor in practice. In addition, an assessment shall be made of whether the traditional allocation of responsibility and risk between controller and processor leads to the intended level of protection.

33. SELECTION CRITERIA – Needless to say, it is impossible to document and analyse every possible use case. A selection needs to be made. In the first phase of selection, a preliminary literature study will be undertaken to identify eligible use cases. The threshold for eligibility shall be the existence of some indication, either in regulatory guidance or doctrine, that the use case in question challenges either the application of

the controller and processor concepts or the allocation of responsibility and risk among actors involved in the processing of personal data. Once the initial screening for relevancy is completed, a further selection will be made with the aim of ensuring a sufficient degree of variation on the dimensions of theoretical interest and ensuring representativeness.[44]

34. SCOPE – The choice has been made to use the controller-processor model of Directive 95/46, rather than that of the GDPR, as the relevant legal framework during the analysis of use cases. There are mainly two motivations behind this approach. First, in doing so, it is possible to create a better understanding of the policy choices made by the European legislature in the context of the GDPR, which will be analysed in Part V. Second, this approach will facilitate the evaluation of whether the approach adopted by the GDPR is likely to remedy the issues which challenged the controller processor-model under Directive 95/46 or whether additional improvements may be necessary.

35. METHODOLOGY – Each of the selected uses cases will be analysed in a structured and focused manner.[45] First, an overview of the main types of actors and interactions will be provided. Next, the legal status and obligations of each actor shall be analysed, taking into account the different interpretations put forward by courts, regulators and scholars. Finally, at the end of each use case, an evaluation will be made of the main issues that have been identified when applying the controller-processor model to the use case in question. The identified issues will serve as the main input for the typology of issues developed in Part V.

4 RECOMMENDATIONS

36. RESEARCH OBJECTIVE – Part V of the thesis aims to provide normative recommendations. Specifically, it aims to provide recommendations as to how the current allocation of responsibility and risk among actors involved in the processing of personal data might be modified in order to increase legal certainty while maintaining at least an equivalent level of data protection.

37. METHODOLOGY – The method used to articulate normative recommendations consists of four steps. First, the issues identified in Part IV shall be categorised and presented in a structured manner (typology of issues). Second, an inventory will be made of ways in which these issues might be remedied (typology of solutions). Third, an

[44] See also J. Seawright and J. Gerring, "Case Selection Techniques in Case Study Research – A Menu of Qualitative and Quantitative Options", *Political Research Quarterly* 2008, Vol. 61, No. 2, p. 296.

[45] The analysis shall be "structured" in the sense that the analysis of each use case will be composed of the same subsections and answer the same questions in relation to each use case. The analysis shall be "focused" in that the analysis shall extend only to those aspects which are relevant for purposes of the research question which this Part seeks to address. Based on A.L. George and A. Bennet, *Case Studies and Theory Development in the Social Sciences*, *o.c.*, p. 67 et seq.

evaluation will be made of the extent to which the proposed remedies are capable of addressing each of the identified issues. The evaluation of possible solutions shall, for the most part, be based on the typology of issues. Each proposal will be evaluated on the basis of whether, and if so, to what extent, it is capable of addressing each of the identified issues.[46] If multiple solutions have been proposed to remedy a particular issue, an internal comparison will be made. Where appropriate, insights from the field of law and economics will be applied to assist the internal comparison of the proposed solutions.[47] Finally, the approach adopted by the European legislature in the context of the GDPR will be compared with the outcome of the preceding evaluations. Where relevant, recommendations for possible further improvements will be made.

[46] In other words, the development of normative recommendations shall be based on the evaluation of possible solutions and their ability to address the identified issues, as opposed to on the basis of abstract principles. As will be seen, however, certain abstract principles (e.g., legal certainty, effective and complete protection) have been involved in the identification of issues. As the typology issues shall act as a positive assessment framework, the relevant principles shall be incorporated in the analysis.

[47] In other words, the typology of issues shall serve as the positive assessment framework to evaluate the proposed solutions. No additional assessment criteria will be used to evaluate the proposed solutions. Only in the context of the internal comparison of possible solutions, shall the insights from the field of law and economics be applied in order to enhance the evaluation process.

PART II

DIRECTIVE 95/46

Chapter 1 INTRODUCTION

38. PREFACE – At the moment of writing, the main legal instrument on data protection in the EU is still Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[48] This Directive – implemented into national law across the EEA – formulates the basic principles and rights of data subjects in relation to the processing of their personal data.[49]

39. OUTLINE – Over the following chapters, the regulatory scheme of Directive 95/46 will be analysed. After describing its scope of application and basic protections, a detailed analysis will be made of how Directive 95/46 allocates responsibility and risk among actors involved in the processing of personal data. First, the key elements of the concepts of controller and processor shall be elaborated. Next, the relationship between controllers, co-controllers and processors will be discussed, followed by an analysis of the liability exposure of each actor. Finally, a number of specific issues relevant to the practical application of the controller and processor concepts shall be discussed.

40. METHODOLOGY – The analysis over the following chapters is based in first instance on the text of Directive 95/46, its preparatory works and the guidance issued by the Article 29 Working Party. In certain places, however, the analysis is supplemented by insights offered by the preparatory works which accompanied national implementations of Directive 95/46. The research hypothesis underlying this approach is that national deliberations on the topic of how Directive 95/46 should be implemented into national law can yield additional insights as to how policymakers understood the provisions of Directive 95/46 at the time of its enactment.[50] Finally, as regards the liability exposure of controllers and processors, reference shall also be made to the Principles of European Tort Law (PETL) as well as national Belgian tort law. The reason for doing so is that Directive 95/46 does not exhaustively harmonise the liability exposure of controllers and processors. By incorporating these supplemental sources into the analysis, however, it is possible to complement the analysis of Directive 95/46 with a number of important elements.

---

[48] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, *O.J.* 23 November 1995, L 281/31–50, hereafter also referred to as "Directive 95/46/EC" or simply "the Directive".

[49] B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *Global Identity Networking for Individuals* (GINI), Deliverable D3.1, 2011, p. 14, available at http://www.gini-sa.eu (last accessed 18 April 2016).

[50] The preparatory works accompanying the following national laws were consulted: France, Netherlands, Belgium and UK. The reason why the analysis of preparatory works to these national implementations of Directive 95/46 is simply because they are written in languages which I am fluent. After consultation, however, it appeared that mainly the preparatory works of the Dutch and Belgian data protection acts offered additional insights which merited inclusion.

Chapter 2 SCOPE

41. RATIONE MATERIAE – Directive 95/46/EC applies to "*the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*" (art. 3(1)).

42. PERSONAL DATA – Article 2(a) defines personal data as "*any information relating to an identified or identifiable natural person ('data subject')*". The concept of "personal data" is extremely broad. Any type of information that pertains to an individual is considered personal data. For example, not only text, but also photos qualify as personal data. Even sound can qualify as personal data.[51]

43. IDENTIFIABILITY – For Directive 95/46 to apply, the data must pertain to an identified or identifiable (natural) person. A person is considered "identifiable" if he or she "*can be identified, either directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". To determine whether or not a person is identifiable, one should take into account all the means which reasonably might be used to identify the data subject.[52] Additional elements that might be taken into consideration when evaluating whether or not the data subject is identifiable are for instance the type of information, the knowledge which one has already, the structure of the data set, the available techniques, the nature of the data and the number of characteristics that are processed.[53]

44. PROCESSING – Article 2(b) defines the "processing of personal data" as

> "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*"

Similar to the definition of "personal data", the definition of "processing" under the Directive 95/46 is also extremely broad. *Any* operation performed upon personal data

---

[51] D. De Bot, *Verwerking van persoonsgegevens, Antwerpen*, Kluwer, 2001, 23. See also C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 91-98.

[52] Recital (26) of Directive 95/46/EC. See also Article 29 Working Party, Opinion 4/2007 on the concept of personal data", WP 136, 20 June 2007, p. 15-17, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (last accessed 25 April 2016). See also the Opinion of Advocate-General Campos Sánchez-Bordana in *Breyer*, C‑582/14, ECLI:EU:C:2016:339, at paragraphs 63-78.

[53] S. Callens, *Chapters on pharmaceutical law*, Antwerpen, Intersentia, 2000, 167-168. See also Article 29 Working Party, Opinion 4/2007 on the concept of personal data", *l.c.*, p. 12-13.

by automatic means is covered by the definition of processing.[54] With regards to non-automated processing, Directive 95/46 only applies to the extent that the personal data is included in a filing system or intended to be part of filing system (article 3(1)).

45. EXEMPTIONS – The scope of the Directive covers all automated processing of personal data, save for the areas excluded by article 3(2) of the Directive, namely the processing of personal data:

(1) *"in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law; and*

(2) *by a natural person in the course of a purely personal or household activity*."

[54] See also C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 98-99.

Chapter 3 BASIC PROTECTIONS

46. OUTLINE – Directive 95/46 seeks to protect individuals with regard to the processing of their personal data by (1) requiring compliance with a number of basic principles; (2) providing individuals with a right to information as well as other data subject rights; (3) imposing an obligation to ensure the confidentiality and security of processing; (4) requiring the establishment, at national level, of supervisory authorities dedicated to monitoring compliance with the substantive provisions of Directive 95/46.

1 PRINCIPLES CONCERNING THE PROCESSING OF PERSONAL DATA

47. FAIRNESS AND LAWFULNESS – Article 6(1)a provides that personal data must be processed "*fairly and lawfully*". Fairness of processing is considered an overarching principle of data protection law.[55] It is a generic principle which has provided the foundation for other data protection requirements. As such, the fairness principle provides a "lens" through which the other provisions in the Directive should be interpreted.[56] The principle of lawfulness of processing reaffirms that data controllers must stay in line with other legal obligations, even outside of the Directive, regardless of whether these obligations are general, specific, statutory or contractual.[57]

48. FINALITY – Article 6(1)b of Directive 95/46/EC dictates that personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*." This provision embodies the so-called "*principle of finality*", which comprises two basic rules. First, it requires controllers to clearly articulate the purposes for which personal data are being collected (purpose specification).[58] Second, it requires controllers to limit their subsequent use of this

---

[55] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, Kluwer International 2002, Den Haag, p. 58. See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *ICRI Working Paper Series*, Working paper 15/2013, September 2013, p. 31.

[56] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 31. See also A. Kuczerawy and F. Coudert, "Privacy Settings in Social Networking Sites: Is It Fair?," in *Privacy and Identity Management for Life*, 2011, p. 237–238 ("*The collection and processing of personal data must be performed in a way that does not intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity*") with reference to L.A. Bygrave, *Data Protection Law, Approaching its rationale, logic and limits, o.c.*, p. 58. The open-ended nature of the fairness principle seems to place a general obligation on controllers to act in a responsible way. This requirement becomes particularly relevant in situations where the extent to which data subjects can exercise control over the processing is limited (e.g., because of a significant power imbalance between controllers and subjects, because of the complexity of processing, etc.). (B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 31.)

[57] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after Google Spain: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 31.

[58] *Ibid*, p. 32.

information to practices compatible with the purposes defined at the moment of collection (use limitation).[59] By defining the purpose at the outset, the data controller establishes the benchmark against which the other data quality principles will be measured.[60] This makes it possible to assess the fairness, lawfulness and proportionality of processing, as well as to evaluate the data controller's compliance with the use limitation principle.[61]

49. LEGITIMACY – The purposes of the processing must not only be specified, it must also be legitimate. The EU Data Protection Directive 95/46/EC restricts the instances in which the processing of personal data may take place. In particular, article 7 enumerates several legal grounds, of which at least one must be present in order for the processing of personal data to be legitimate (e.g., data subject consent, necessity for the performance of a contract, etc.).[62]

50. PROPORTIONALITY – Article 6(1)c specifies that the processing of personal data should be limited to data that are "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*".[63] Article 6(1)c requires that there exists a sufficiently narrow correlation, in terms of both adequacy and relevancy, between the legitimate purpose articulated by the controller and the data being collected. Moreover, only data which are necessary to achieve the legitimate aims

---

[59] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 32. See e.g. Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", WP 203, 2 April 2013, 70 p., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; L.A. Bygrave, "Core principles of data protection", *Privacy Law and Policy Reporter*, vol. 7, issue 9, 2001; E. Kosta and J. Dumortier, "The Data Retention Directive and the principles of European Data protection legislation", *Medien und Recht International*, issue 3, 2007, p. 133; C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 99-100 and D. Elsegem, "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data", *Ethics and Information Technology* 1999, vol. 1, p. 287-288..

[60] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 32.

[61] *Id.* and S. Gutwirth, *Privacy and the information age*, *o.c.*, p. 97-102. See also Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 33, with reference to M.-H. Boulanger, C. De Terwangne, T. Léonard, S. Louveaux, D. Moreau and Y. Poullet, "La Protection des Données à caractère personnel en droit communautaire", *Journal de Tribunaux Droit Européen* 1997, p. 127 and 145-147; D. De Bot, *Verwerking van persoonsgegevens, o.c.*, p. 118-121 and T. Léonard, "La protection des données à caractère personnel et l'entreprise", Brussels, Kluwer, 2004, livre 112.1, p. 29.

[62] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 33, with reference to M.-H. Boulanger, C. De Terwangne, T. Léonard, S. Louveaux, D. Moreau and Y. Poullet, "La Protection des Données à caractère personnel en droit communautaire", *l.c.*, p. 147-148. See also L.A. Bygrave, *Data Protection Law, Approaching its rationale, logic and limits, o.c.*, p. 61-62 and C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, second edition, Oxford University Press, New York, 2007, p. 74-46 and p. 90.

[63] This provision is generally considered a manifestation of a more general data protection principle, namely the principle of proportionality. (B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 33). For a more comprehensive overview of the role of the proportionality principle in the Data Protection Directive and EU law in generals see C. Kuner, "Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies", *Privacy & Security Law Report* 2008, vol. 07, no. 44, p. 1615. See also B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.,* p. 25-27.

of the controller may be processed.[64] Article 6(1)c further provides that personal data may not be kept in a form which permits identification of data subjects for longer than necessary to realise for the purposes for which the data were collected (or for which they are further processed).

51. ACCURACY – Every controller is under the obligation to ensure the accuracy of the personal data it processes (article 6(1)d). This provision in first instance requires controllers to put in place mechanisms and procedures which enable them to establish the accuracy of data with a level of assurance proportionate to the interests at stake. Article 6(1)d of the Directive also stipulates that data must be kept up-to-date where necessary. This implies that controllers are in principle obliged to meet the requirement of accuracy not only at the moment of collection, but as long as the data is being processed under their control.[65]

52. SENSITIVE DATA – Finally, it is worth noting that article 8 of Directive 95/46 imposes additional restrictions regarding the processing of so-called "sensitive" categories of data, which include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2 TRANSPARENCY AND DATA SUBJECT RIGHTS

53. OUTLINE – Articles 10 et seq. of Directive 95/46/EC set forth the transparency obligations of controllers and list the rights data subjects can exercise towards controllers when their personal data is being processed. Underlying these provisions is the idea that the data subject should in principle:

(a) be notified of the processing of her personal data (right to information);

(b) have means to obtain further information (right of access); and

(c) have immediate means of recourse towards the controller in case she feels her data are being processed improperly (right to rectification, erasure or blocking).[66]

---

[64] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 33, with reference to M.-H. Boulanger, C. De Terwangne, T. Léonard, S. Louveaux, D. Moreau and Y. Poullet, "La Protection des Données à caractère personnel en droit communautaire", *l.c.*, p. 147. See also D. De Bot, *Verwerking van persoonsgegevens, o.c.*, p. 124-125.

[65] B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 22.

[66] *Ibid*, p. 28. See also B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", *International Review of Law, Computers & Technology* 2013, available at http://www.tandfonline.com/doi/pdf/10.1080/13600869.2013.812594 (last accessed 25 April 2016) and Bygrave, *Data Protection Law, Approaching its rationale, logic and limits, o.c.*, p. 63-66.

54. DUTY TO INFORM – Articles 10 and 11 of the Directive specify which types of information controllers must provide to data subjects with regards to the processing of their personal data.[67] As a rule, each data subject must be informed of at least the identity of the controller (and, if applicable, of his representative) and the purposes of the processing.[68] In addition, the Directive stipulates that Member States must require controllers to provide the data subject with supplemental information "*in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected , to guarantee fair processing in respect of the data subject*".[69] Such additional information can refer to the recipients or categories of recipients of the data, information with regard to the existence of the right of access, the right to rectify inaccurate data, etc.[70]

55. RIGHT OF ACCESS – Article 12 stipulates that every data subject shall have the right to obtain from the controller, without constraint, at reasonable intervals and without excessive delay or expense:

(a) confirmation as to whether or not data relating to her are being processed;

(b) information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

(c) communication to her in an intelligible form of the data undergoing processing and of any available information as to their source; and

(d) knowledge of the logic involved in any automatic processing of data concerning her at least in the case of the automated decisions.

56. RECTIFICATION, ERASURE OR BLOCKING – Article 12(b) of the Directive stipulates that data subjects shall have the right to obtain, as appropriate, the "rectification, erasure or blocking" of data in case where the processing of which does not comply with the provisions of the Directive. Rectification shall be particularly appropriate in instances where the data being processed is found to be inaccurate.

---

[67] Articles 10 and 11 address two different scenarios, respectively: one in which the information is obtained directly from the data subject (art. 10), and one in which the information is collected indirectly (i.e. from an entity other than the data subject) (art. 11). The duty to inform is similar in both scenarios; the main relevance of the distinction concerns (a) the moment by which notice must be provided and (b) the exemptions to the notice provision.

[68] The use of plural "purposes", in Articles 10–11, implies that the data subject has to be informed not only about the main purpose to be accomplished, but also about any secondary purposes for which the data will be used. (B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", *l.c.*, at note 7.)

[69] Articles 10-11(1)c.

[70] Member State laws vary considerably with regard to the kinds of information that must actually be provided in order to ensure fairness of processing. Sometimes the examples given in the Directive are repeated, other times somewhat different examples are included, and sometimes there are no examples at all. See Article 29 Data Protection Working Party, "Opinion on More Harmonised Information Provisions", WP100, 25 November 2004, p. 3. (B. Van Alsenoy, E. Kosta and J. Dumortier, "Privacy notices versus informational self-determination: Minding the gap", *l.c.*, at note 9.)

However, this provision also enables data subjects to request the deletion or blocking of data where it appears the data has been obtained unlawfully or there is no longer a legitimate need to maintain the data.[71] In instances where the data subject's request for amendment, deletion or blocking is granted, she may also request that controller provides notification thereof to any third parties to whom the data have been disclosed. The only grounds for the controller to refuse such a request would be to assert that such notification is impossible or involves a disproportionate effort (art. 12(c)).[72]

3 CONFIDENTIALITY AND SECURITY

57. BASIC PRINCIPLE – Articles 16 and 17 of Directive 95/46/EC oblige the controller(s) of a processing operation to implement appropriate technical and organisational measures to ensure the confidentiality and security of processing. In particular, controllers must adopt appropriate measures to "*protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access [...] and against all other unlawful forms of processing.*" The controller's security obligation is defined as an obligation of means. There are four criteria for determining the extent of this obligation, namely state-of-the-art, cost, the risks presented by the processing, and the nature of the data to be protected (article 17(1)).[73] The general security obligation of controllers can be broken down into a number of components, each of which corresponds with one or more security objectives.[74]

58. CONFIDENTIALITY – A first security objective following from the controller's security obligation is to maintain the confidentiality of information. Confidentiality as a security objective can be described as keeping the content of information secret from all parties except those that are authorized to access it.[75] There are numerous approaches to providing confidentiality, ranging from physical protection to the use of access control and cryptographic algorithms.[76] In addition to safeguarding the confidentiality of information, the processing capabilities (read, write, modify ...) of each party should be limited to that which is necessary to realize the goals of the processing. This follows from a combined reading of the controller's security obligation and the proportionality

[71] B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 38.
[72] *Ibid*, p. 30.
[73] B. Van Alsenoy, E. Kindt and J. Dumortier, "Privacy and data protection aspects of e-government identity management", in S. Van der Hof, M.M. Groothuis (eds.), *Innovating Government - Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series (IT & Law), Vol. 20, T.M.C. Asser Press, Springer, 2011, p. 257.
[74] B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 30.
[75] X. Huysmans and B. Van Alsenoy (eds.), "Conceptual Framework – Annex I. Glossary of Terms", *IDEM*, Deliverable D1.3, v1.07, 2007, p. 12.
[76] J.C. Buitelaar, M. Meints and E. Kindt, "Towards requirements for privacy-friendly identity management in eGovernment", *FIDIS*, Deliverable D16.3, 2009, p. 19.

principle. These requirements apply not only at the level of each organisation, but also at the level of each individual user.[77]

59. INTEGRITY AND AUTHENTICITY – Data controllers are required to integrate appropriate security policies to safeguard the integrity and authenticity of the data. Integrity as a security objective is understood as ensuring data has not been altered by unauthorized or unknown means.[78] Authenticity as a security objective is generally understood as verifiable assurance that data has emanated from the appropriate entity and has not been altered by unauthorized or unknown means (and thus the "authenticity" of data also implies data integrity).[79]

60. AVAILABILITY – Data controllers are under the obligation to protect personal data against accidental destruction or loss. This requirement can be approximated to the security objective of availability, which can be described as the property of being accessible and useable upon demand by an authorized entity.[80]

61. CATCH-ALL – Finally, it is worth noting that article 17(1) of the Directive also contains a generic obligation to take appropriate organisational and technical measures to protect personal data against "all other unlawful forms of processing". This provision may be interpreted as requiring controllers to take all reasonable precautions to mitigate the risk of unauthorized processing activities by third parties or insiders.[81]

4 SUPERVISORY AUTHORITIES

62. BASIC PRINCPLE – Article 28 of Directive 95/46 requires Member States to have in place an independent supervisory authority which is dedicated to monitoring compliance. Each supervisory authority must be endowed with (a) investigative powers; (b) effective powers of intervention[82]; and (c) the power to engage in legal proceedings where the national provisions adopted pursuant to the Directive have been violated or to bring these violations to the attention of the judicial authorities.[83] Every individual

[77] *Ibid*, p. 20. See also B. Van Alsenoy, E. Kindt and J. Dumortier, Privacy and data protection aspects of e-government identity management", *l.c.*, p. 258.
[78] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997, p. 3.
[79] *Ibid*, p. 25.
[80] ITU-T SG 17, "Security Compendium. Part 2 – Approved ITU-T Security Definitions", 13 May 2005, available at http://www.itu.int/ITU-T/studygroups/com17/def005.doc (last accessed 25 April 2016).
[81] B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 32.
[82] Examples include the delivering opinions before processing operations are carried out, in accordance with Article 20 of Directive 95/46 and ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
[83] Article 28(3) of Directive 95/46.

who feels his or her rights and freedoms are being harmed by the processing of personal data has the right to file a complaint with a supervisory authority.[84]

63. ARTICLE 29 WORKING PARTY – Article 29 of Directive 95/46 calls for the creation of a "Working Party", composed of a representative of the supervisory authority or authorities designated by each Member State. The mission of the Working Party is

(a) examine any question covering the application of the national measures adopted under Directive 95/46 in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.[85]

[84] Article 28(4) of Directive 95/46.
[85] Article 30(1) of Directive 95/46.

Chapter 4 ALLOCATION OF RESPONSIBILITY AND RISK

64. OUTLINE – Directive 95/46/EC assigns responsibility for compliance with its provisions to the "controller" of the processing. It also contains the concept of a "processor", as a means to address the situation where a controller enlists another actor to process personal data on its behalf. Given the central importance of these concepts to the research question of this thesis, it is necessary to analyse the meaning of these concepts in some detail. The following subsections will analyse

(1) the key elements of the controller and processor concepts;

(2) the legal relationship between controllers and processors;

(3) the legal relationship between (co-)controllers;

(4) the liability exposure of (co-)controllers and processors; and

(5) a selection of specific issues.

1 KEY ELEMENTS OF THE "CONTROLLER" AND "PROCESSOR" CONCEPTS

65. PRELIMINARY REMARKS – With the adoption of Directive 95/46, the key principles for allocating responsibility and risk for data processing were established. How these principles were to be applied in practice, would be determined by a steadily growing body of materials (opinions, recommendations, enforcement actions) developed by national data protection authorities. For quite some time, only limited EU-wide guidance existed on how to apply the concepts of "controller" and "processor" practice. While the Article 29 Working Party was called upon to interpret these concepts in relation to specific cases, the resulting guidance was generally closely tied to the specific issue at hand.[86]

66. OPINION 1/2010 – In 2010, the Article 29 Working Party published an Opinion on the concepts of "controller" and "processor".[87] The main motivation for the Opinion

[86] See e.g. "Working Document on online authentication services", WP68, 29 January 2003 (available athttp://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp68_en.pdf); "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", WP128, 22 November 2006 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf); "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", WP140, 20 September 2007 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_en.pdf); "Opinion 5/2009 on online social networking", WP163, 12 June 2009 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf).

[87] Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor"", WP 169, 16 February 2010, 31 p., accessible at

was a desire to promote a consistent and harmonized approach in the interpretation of these concepts among the Member States.[88] The Working Party had noticed that practitioners in different Member States exhibited different interpretations, at least as to certain aspects of these concepts.[89] In addition, the Working Party had also observed that the concrete application of the concepts controller and processor was becoming increasingly complex, mostly due to increasing complexity of the environments in which these concepts are used.[90]

67. OUTLINE – Opinion 1/2010 of the Article 29 Working Party represents the most comprehensive attempt to clarify the meaning of the "controller" and "processor" concepts to date. Given the authority enjoyed by WP29 opinions, as well as their strategic importance, Opinion 1/2010 will serve as the main source of reference to further elucidate the key elements of the controller and processor concepts over the following sections.

1.1 CONTROLLER

68. CONTROLLER – A controller is defined by article 2(d) of Directive 95/46 as

> *"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".

69. "ANY BODY" – Under Directive 95/46/EC, a controller can be "a natural or legal person, public authority, agency or any other body".[91] This means that there is in principle no limitation as to which type of actor might assume the role of a controller. It might be an organisation, but it might also be an individual or group of individuals.[92]

70. "DETERMINES" – A second key element of the controller concept refers to the controller's *factual influence* over the processing, by virtue of an *exercise of decision-*

---

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (last accessed 1 September 2015).

[88] *Ibid*, p. 3.

[89] *Ibid*, p. 2.

[90] *Ibid*, p. 2 and 6.

[91] This portion of the controller definition is identical to that the definition of a data controller in both the OECD Guidelines and Convention 108. Cf. *infra*; nr. 365 and nr. 397. See also Opinion 1/2010, *l.c.*, p. 15. According to the Working Party, this portion of the definition was simply assimilated from article 2 of Convention 108 and was not the object of any specific discussion during the preparation of Directive 95/46/EC (*Id.*).

[92] According to the Article 29 Working Party, it is generally better to consider a company or organisation as a controller rather than a specific person within a company or organisation. See Opinion 1/2010, *l.c.*, p. 15. The extent to which individuals within organisations might be considered as controllers will be discussed *infra*; nrs. 151 et seq.

making power.[93] In order to assess which actor(s) wield(s) relevant factual influence over the processing, one should look at the entirety of factual elements surrounding the processing. Useful questions to ask at this stage include: "*Why is this processing taking place?*" and "*Who initiated it*?"[94]

71. "PURPOSES AND MEANS" – The third key element of the controller concept refers to the object of the controller's influence, namely the "purposes and means" of the processing. The Article 29 Working Party has paraphrased this portion of article 2(d) by saying that the controller is the actor deciding about *the "why" and the "how"* of the processing:[95] given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., "to what end"; or "what for") and *how* this objective shall be reached (i.e., which means shall be employed to attain the objective).[96]

72. "ALONE OR JOINTLY WITH OTHERS" – Article 2(d) recognizes that the "purposes and means" of the processing might be determined by more than one actor. It alludes to this possibility by stating that the controller is the actor who "alone or jointly with others" determines the purposes and means of the processing.[97] The extent to which two or more actors jointly exercise control may take on different forms, as will be clarified later on.[98]

73. "OF THE PROCESSING OF PERSONAL DATA" – The purposes and means determined by the controller must relate to the "processing of personal data". Article 2(b) of the Directive defines the processing of personal data as "*any operation or set of operations which is performed upon personal data*". As result, the concept of a controller can be linked either to a single processing operation or to a set of operations. According to the Article 29 Working Party, the question of which party is acting as a controller should be looked at "*both in detail and in its entirety*".[99]

74. "DESIGNATED BY NATIONAL OR COMMUNITY LAW" – Finally, it is worth observing that article 2(d) explicitly foresees that a "controller" might also be designated through national or community law, particularly in situations "*where the*

[93] Opinion 1/2010, *l.c.*, p. 8-9
[94] *Ibid*, p. 8.
[95] See also Opinion 1/2010, *l.c.*, p. 13.
[96] Of the two objects of the controller's influence, regulators appear to place greater weight on the controller's determination of finality ("purpose") than upon his determination of "means". This aspect will be discussed in greater detail *infra*; nrs. 92et seq.
[97] See also T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 419.
[98] Cf. *infra*; nrs. 101 et seq.
[99] Opinion 1/2010, *l.c.*, p. 3 and 20-21. See also *infra*; nr. 99 and 466.

purposes and means of processing are determined by national or Community laws or regulations".[100]

1.2 PROCESSOR

75. DEFINITION – A processor is defined by article 2(e) as

"*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*"

76. "ANY BODY"– Similar to the definition of a controller, the definition of a processor envisages a broad range of actors: any natural or legal person, public authority, agency "or any other body" can assume the role processor.[101] The only requirement in this respect is that the actor in question is separate from the controller.[102]

77. "ON BEHALF OF" – The main substantive component of the processor concept is that a processor acts "on behalf" of a controller. The Article 29 Working Party has approximated this wording with the legal concept of *delegation*, whereby one party requests another party to undertake certain actions on its behalf.[103] The term "delegation" is often used in reference to figures of legal representation.[104] The term can also be used, however, to refer to the process whereby one party requests another party to perform one or more actions of a non-legal nature. The Working Party appears to have used the term "delegation" in the latter sense, as the type of services typically associated with processors consist mainly in the performance of technical operations.[105]

78. IN ACCORDANCE WITH INSTRUCTIONS – In order for an actor to be qualified as a "processor" rather than a "controller", it is required that the actor is processing personal data pursuant to someone else's instructions (i.e. the instructions issued by the controller). Although this is not explicitly mentioned in the definition of a "processor", it

---

[100] See also *infra*; nr. 167.
[101] See also Opinion 1/2010, *l.c.*, p. 24.
[102] *Ibid*, p. 25.
[103] *Id.*
[104] In the case of legal representation, one party (the principal) bestows upon another party (the agent), the authority to undertake one or more legal actions on the principal's behalf. (See O. Lando and H. Beale (eds.), *Principles of European Contract Law - Parts I and II*, prepared by the Commission on European Contract Law, The Hague, Kluwer Law International, 2000, 197 et seq.) The legal effects of these actions shall, as a rule, be attributed directly to the principal (provided the agent acts with in the scope of his authority). Even where the agent exceeds his authority, his actions might still be attributed to the principal under the theory of apparent authority. For more information see also B. Van Alsenoy, D. De Cock, K. Simoens, J. Dumortier and B. Preneel, "Delegation and digital mandates: Legal requirements and security objectives", *Computer, Law and Security Review* 2009, Vol. 25, no 5, p. 415-420.
[105] Of course, a processor might also perform legal acts on behalf of a controller, e.g. in case of further subcontracting pursuant to the instructions of the controller; or where the processor also operates the front-office for consent registration and acceptance of the terms of use of a particular service.

follows from a combined reading of article 2(e) articles 16-17 of Directive 95/46/EC.[106] The latter set of provisions regulates the legal relationship between controller and processors, which shall be further elaborated in the course of the following subsection.

2 RELATIONSHIP BETWEEN CONTROLLERS AND PROCESSORS

2.1 BOUND BY INSTRUCTIONS

79. BASIC PRINCIPLE – Article 16 of the Directive provides that

> *"any person acting under the authority of the controller or of the processor, including the processor himself, [...] must not process them except on instructions from the controller, unless he is required to do so by law*".

Article 16 can be explained by the fact that the Directive bestows upon the controller the duty to ensure compliance. Because the processor is seen as a mere "delegate" of the controller, it would arguably undermine the effectiveness of the regulatory framework if a processor were free to process data beyond the instructions received from the controller. [107] The heading of article 16 refers to "confidentiality of processing". Strictly speaking, the heading is too narrow, as article 16 refers not only to unauthorized disclosure but any form of unauthorized processing.[108] For example, unauthorized deletion of personal data would also constitute a violation of article 16.[109]

80. NOT A "SUBORDINATE" OF THE CONTROLLER – While the processor is legally prohibited from processing the data "except on the instructions of the controller", he is not necessarily a "subordinate" of the controller.[110] A processor is typically an independent contractor, who is not in a hierarchical relationship with the controller.[111]

---

[106] In the same vein: Commissie voor de Persoonlijke Levenssfeer, Decision of 9 December 2008 regarding the Control and recommendation procedure initiated with respect to the company SWIFT, at paragraph 120 available at https://www.privacycommission.be/sites/privacycommission/files/documents/swift_decision_en_09_12_2008.pdf (last accessed 30 April 2016).

[107] See also U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, 1997, Baden-Baden, Nomos Verlagsgesellschaft, p. 224. Within the logic of Directive 95/46, the legitimacy of an entity"s processing activities as "processor" is determined by the mandate given by a controller (who is considered ultimately responsible for ensuring the legitimacy of processing). If a processor goes beyond the scope of its instructions, it would lose its legal status of "processor" (because it would then no longer be processing data "on behalf of" the controller). Its legal status would in principle then change from that of a "processor" to that of a "controller" or "co-controller". See also Opinion 1/2010, *l.c.*, p. 25.

[108] U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 224.

[109] *Id.*

[110] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, Vergaderjaar 1997-1998, 25 892, nr. 3, p. 61.

[111] *Id.*

81. DEGREE OF AUTONOMY – In practice, processors enjoy considerable discretion in deciding how to organize their services.[112] This gives rise to the following question: to what extent may an actor influence the processing before it can no longer be considered a mere "processor"? According to the Article 29 Working Party, processors can enjoy a certain degree of autonomy when processing personal data on behalf of others. Specifically, the Working Party accepts that a processor has a certain "margin of manoeuvre" in deciding how the processing shall be organized.[113]

2.2 DUE DILIGENCE

82. CHOICE OF PROCESSOR – Article 17(2) stipulates that

> "*The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.*"

83. VETTING – Article 17(2) essentially requires controllers to exercise appropriate care when selecting a processor. Specifically, it requires them to ascertain whether the processor provides sufficient guarantees in respect of the "technical security and organisational measures" that will govern the processing to be carried out. The selection of an appropriate processor shall generally be easier if the processor specifies the level of security being kept by him with reference to an external security standard.[114] Absent such an indication, the controller must himself assess whether the processor provides sufficient guarantees in respect of the processing to be carried out (although he may of course engage an external expert to make the assessment for him).[115]

84. OVERSIGHT – Article 17(2) also requires controllers to ensure that processors in fact live up to their commitments. Simply obtaining copies of the processor's security policies is not sufficient.[116] The controller must also verify that the relevant measures are in fact implemented in practice.[117] It is not required that the controller conducts such a verification in person. The controller may also rely upon the assessment of an external expert or upon information provided by a supervisory authority.[118] Finally, it is worth noting that the duty to ensure that the processor complies with the relevant measures is an ongoing obligation. In other words, the controller must verify proper implementation not only when he first enlists the processor, but throughout the entire

---

[112] One of the main reasons why organisations outsource certain processing activities is precisely because they do not have the requisite expertise in-house. By definition such outsourcing arrangements imply that the service provider will enjoy certain discretion in deciding how the processing will be organised.
[113] Opinion 1/2010, *l.c.*, p. 13-14. See also *infra*; nrs. 93 et seq.
[114] U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 230.
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *Id.*

duration of the processing.[119] The controller should therefore ensure periodic validation in case of processing contracts which span a longer a period of time.[120]

2.3 LEGAL BINDING

85. "CONTRACT OR OTHER LEGAL ACT"– Article 17(3) of the Directive obliges controllers to put in place a contract or other legal act "binding the processor to the controller", which must specify that the processor is obliged (1) to follow the controller's instructions at all times and (2) to implement appropriate technical and organisational measures to ensure the security of processing.[121] Specifically, article 17(3) provides that

> "*The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
> *- the processor shall act only on instructions from the controller,*
> *- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.*"

Article 17(3) only mentions the minimum content that should be included in an arrangement between controllers and processors. According to the Working Party, the contract or other legal act should additionally include "*a detailed enough description of the mandate of the processor*".[122] In practice, the legal act binding the processor to the controller shall most often take the form of a contract. The reference to "other" legal acts in article 17(3) mainly concerns the public sector, where a processor might be appointed either directly by way of legislation or by way of a unilateral decision of a public body.[123]

86. IN WRITING OR EQUIVALENT FORM – Finally, article 17(4) specifies that

> "*For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the [security measures] shall be in writing or in another equivalent form"*.

Article 17(4) explicitly states that the obligation to lay down the contract or legal act in writing or equivalent from is imposed "*for the purposes of keeping proof*".[124] The

---

[119] *Id.* If there is reason to suspect that the security measures are no longer adequate (e.g., in case of a security breach), the controller must undertake the necessary steps to ensure that an appropriate level of security is reinstated. If he is not able to remove all doubts, he must end his contract with the processor and demand that the data be provided back to him. (*Id.*)
[120] *Id.*
[121] Opinion 1/2010, *l.c.*, p. 26.
[122] *Id*. See also U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 232 (noting that the contract or legal act should generally address all data protection issues including, for example, how to deal with access requests by governments or other interested third parties).
[123] U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 231.
[124] *Ibid.* p. 232.

presence (or absence) of a written arrangement is therefore not decisive for the existence of a controller-processor relationship.[125] Where there is reason to believe that the contract does not correspond with the reality in terms of actual control, the agreement may very well be set aside by the adjudicating body.[126] Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of article 17(4) and provide a first indication that the relationship between the parties is not a controller-processor relationship.

2.4 DISTINGUISHING BETWEEN CONTROLLERS AND PROCESSORS

87. OUTLINE - In Opinion 1/2010, the Article 29 Working Party recognized that it may be difficult to distinguish between controllers and processors in practice.[127] To help guide the application of these concepts, the Working Party developed additional criteria to make it easier for practitioners to determine whether someone is acting as "controller" or "processor". The following paragraphs summarize the main points of guidance provided by the Working Party.

A. Circumstances giving rise to "control"

88. FUNCTIONAL CONCEPT – The concept of a controller is a functional concept: rather than allocating responsibility on the basis of formal criteria, it aims to allocate responsibilities where the factual influence is.[128] This implies that the legal status of an actor as either a "controller" or a "processor" must in principle determined by its actual activities (influence) in a specific context, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract or in a notification to a supervisory authority).[129]

89. NEED FOR PREDICTABILITY – Because the question of "who controls the processing?" is a question of fact, determining who actually controls a particular processing activity may sometimes require an in-depth and lengthy investigation.[130] According to the Article 29 Working Party, however, regulatory effectiveness also requires predictability.[131] Specifically,

---

[125] Opinion 1/2010, *l.c.*, p. 26-27.
[126] *Ibid*, p. 27.
[127] *Ibid*. p. 6
[128] *Ibid*, p. 9.
[129] *Ibid*, p. 25-27. See also Opinion 1/2010, *l.c.*, p. 12: "*the definition of data controller should be considered as a mandatory legal provision, from which parties cannot simply derogate or deviate*". Of course, a formal designation or declaration remains an important factual element which can be taken into account when assessing the legal status of a particular entity, but it is not decisive. (*Id.*) See also *infra*; nr. 163 et seq.
[130] Opinion 1/2010, *l.c.*, p. 9.
[131] *Id.*

"*[…] the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law. This calls for an interpretation of the Directive ensuring that the "determining body" can be easily and clearly identified in most situations, by reference to those - legal and/or factual - circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary.*"[132]

90. CATEGORIES OF CIRCUMSTANCES - According to the Article 29 Working Party, the circumstances which typically give rise to "control" can be classified into three main categories, namely[133]:

a) Control stemming from *explicit legal competence* (e.g., when the controller or the specific criteria for its nomination are designated by national or Community law);

b) Control stemming from *implicit competence*, whereby an analysis of the traditional roles associated with a certain actor will assist in identifying the controller (e.g., an employer in relation to data on his employees, the publisher in relation to data on subscribers); or

c) Control stemming from *factual influence*, whereby the qualification of controller is attributed on the basis of an assessment of factual circumstances which warrant the conclusion that this party exercises a "dominant role" with respect to the processing.

91. ASSESSMENT – The need to ensure predictability of "control" was discussed at length in the context of the preparation of the revisions to the Dutch Data Protection Act of 1989.[134] The Dutch government argued that "control" should in principle be linked to formal competences and criteria (e.g., formal designation, legal authority) as much as possible.[135] Only in cases where multiple actors influence the processing without a clear

---

[132] *Id.*

[133] Opinion 1/2010, *l.c.*, p. 10-12.

[134] See Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, in particular p. 55-57.

[135] The main argument in favor of this approach is that the relationships and power structures between different organisations involved in the processing will generally be opaque towards the data subject. (*Ibid,* p. 15) ("*De formele bevoegdheden zijn duidelijker en dienen daarom het aanknopingspunt te zijn in plaats van de feitelijke machtsverhoudingen met betrekking tot de te verwerken persoonsgegevens. Deze laatste zijn voor de betrokkene minder transparant.*") In response, the Dutch Raad van State pointed out that if the intention of the legislature was to link control to formal competences as much as possible, the definition should also refer to the term "competence" ("*De Raad stelt in de eerste plaats vast dat in dit artikelonderdeel, anders dan de toelichting doet voorkomen, het element bevoegdheid ontbreekt*") (Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Advies Raad van State en Nader rapport", Vergaderjaar 1997–1998, nr. 25 892, p. 4). The Dutch government dismissed the suggestion, however, both to stick as closely as possible to the wording of Directive 95/46 (*ibid*, p. 5) and in order to ensure that entities who undertake to process personal without proper legal authority were brought within the scope of the act (Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming

indication of who the controller is, should the determination of "control" be based on a functional approach. In such instances, responsibility for the processing should above all be determined "*on the basis of generally accepted standards of social interaction*" (in Dutch: "*algemeen in het maatschappelijk verkeer geldende maatstaven*").[136] The Working Party's guidance bears some resemblance to this approach: while recognizing the functional nature of the controller concept, it also tries to link the question of "control" to both formal criteria (e.g., explicit competences) and traditional roles (implicit competences) as much as possible.[137]

B. "Purpose" over "means"

92. THE PRIMACY OF PURPOSE – Article 2(d) defines the controller as the entity which determines both "purposes" and "means" of the processing. Of the two objects of the controller's influence, the Article 29 Working Party places greater weight on the controller's determination of finality ("purpose") than upon his determination of "means".[138] Specifically, the Article 29 Working Party views the determination of purpose(s) as something that is reserved to the controller: whoever decides the purpose acts as a controller.[139] The determination of the "means" of the processing, however, may be (partially) delegated to the processor.[140]

93. SUBORDINATION OF THE "MEANS" CRITERION – As far as the determination of the "means" of the processing is concerned, the Working Party feels that Directive 95/46 supports a certain degree of flexibility. Specifically, it accepts that when a controller relies upon a processor to realize the purpose(s) of the processing, it may leave its processor(s) a certain "margin of manoeuvre" in specifying how the processing shall be organised.[141] In other words, while the determination of purpose "automatically"

---

persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 55) ("*Overeenkomstig artikel 2, onderdeel d, van de richtlijn wordt in de begripsomschrijving niet meer gesproken van de natuurlijke persoon enz. die bevoegd is doel van en middelen voor de verwerking vast te stellen. Indien onbevoegd gegevens worden verwerkt dient immers eveneens een verantwoordelijke te kunnen worden aangewezen en op zijn handelen te kunnen worden aangesproken*.")

[136] *Ibid*, p. 55.

[137] See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, Proefschrift ter verkrijging van de graad van doctor aan de Katholieke Universiteit Brabant, Hilvarenbeek, 1995, p. 400 et seq. (noting that Dutch scholars generally advocate linking control to prevailing norms of social interaction). Interestingly, the cited scholars also conceive of this approach as being a "functional" approach, as it links responsibility for data processing to the function fulfilled by the processing in the relationships between the controller and the data subject (*Ibid*, footnote 1416: "*Het begrip "functioneel" ziet derhalve primair op de functionaliteit van de gegevensverwerking in samenhang met de op overeenkomst en/of de WPR gebaseerde rechts-/informatiebetrekkingen tussen de registratiehouder en de geregistreerde*").

[138] See also P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 539.

[139] Opinion 1/2010, *l.c.*, p. 15.

[140] *Id.*

[141] *Ibid*, p. 13-14.

triggers the qualification of controller, this would not necessarily be the case where an entity only influences the means of the processing.[142]

94. "ESSENTIAL" VS. "NON-ESSENTIAL" MEANS – The margin for manoeuvre accorded to processors is not unlimited. According to the Article 29 Working Party, the influence of the processor may not extend to either the "purpose" or the "essential" means of the processing:

> "*while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means.*"[143]

"Essential means", according to the Working Party, are those elements which are traditionally and inherently reserved to the determination of the controller, such as "*which data shall be processed*?", "*for how long shall they be processed*?", and "*who shall have access to them*?".[144] "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software.[145] Under this approach, the Working Party considers it possible that the technical and organisational means of the processing are determined exclusively by the data processor.[146] A provider of processing services shall only be considered a joint controller if it determines either the purpose or the "essential elements" of the means which characterize a controller.[147]

---

[142] *Ibid*, p. 14.

[143] *Id*.

[144] The Article 29 Working Party derived these criteria from the legislative development of the controller and processor concepts. Previous iterations of the controller concept referred to four elements ("*purpose and objective*", "*which personal data are to be processed*", "*which operations are to be performed upon them*" and "*which third parties are to have access to them*"). Cf. *infra*; nr. 486. According to the Working Party, the word "means" should be understood as comprising these elements. ("*[T]he final definition must rather be understood as being only a shortened version comprising nevertheless the sense of the older version.*") (*Ibid*, p. 14.) See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 57("*Iemand die voor zichzelf verwerkt of doet verwerken, is verantwoordelijke. Hieraan doet niet af dat hij daarmee derden van dienst wil zijn. Van belang is dat hij zelf bepaalt welke soort gegevens hij verwerkt, hoe lang en met welke middelen. Degene daarentegen die krachtens een contract dat blijkens zijn aard betrekking heeft op de gegevensverwerking ten behoeve van een derde, waarbij de wederpartij bepaalt welke gegevens, waartoe, hoelang enz. worden verwerkt, moet worden aangemerkt als bewerker*.")

[145] Opinion 1/2010, *l.c.*, p. 14. The Article 29 Working Party draws a parallel to the figure of delegation, which allows imply a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means. (*Ibid*, p. 25).

[146] *Id.* See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 61-62.

[147] *Ibid*, p. 19. Van Eecke and Truyens point out that the Working Party's distinction between "essential" and "non-essential" means is at odds with the literal wording of article 2(d). (P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 539.) Specifically, they argue that it reduces a dual legal requirement ("and") to a single requirement ("or"), by stating that it is sufficient for a party to determine either the purpose or the essential aspects of the means in order to qualify as a data controller (*Id.*). This criticism is further analysed *infra*; nr. 1093.

95. ASSESSMENT – The tendency to emphasize the purpose over the means of the processing as being determinative for control can also be found in earlier doctrine[148] and regulatory guidance[149]. The weight given to the "purpose" element undoubtedly stems from the fact that "purpose" also fulfils such a central role in determining the scope of a controller's obligations (see in particular article 6(1)b-e; article 7(b)-(f) and articles 10-11).[150]

C. Additional criteria

96. STRONGER "BARGAINING POSITION"? – Article 17(3) obliges the controller to conclude a contract with its processors, which must specify that the processor is to follow the controller's instructions at all times. The phrasing of this provision might suggest that the controller should enjoy a stronger "bargaining position" than its processor. The Working Party has, however, clearly stated that this is not a prerequisite. According to the Working Party, service providers specialized in certain processing of data

> "*will set up standard services and contracts to be signed by data controllers, de facto setting a certain standard manner of processing personal data*".[151]

The mere fact that an entity does not have any other choice than to simply "take it or leave it" does not prevent its qualification as a controller.[152] Along the same line, the Article 29 Working Party has emphasized that the fact that there exists an imbalance in the contractual power of a "small" data controller with respect to "big" service providers does not excuse these "smaller" entities from compliance with data protection law.[153]

97. ADDITIONAL CRITERIA – When it comes to distinguishing between controllers and processors, the Working Party considers the following criteria may be helpful in determining the qualification of the various subjects involved[154]:

(1) *Level of prior instructions given* (the greater the level of instruction, the more limited the margin of manoeuvre of the processor);

(2) *Monitoring of the execution of the service* (a constant and careful supervision of compliance provides an indication of being in control of the processing operations);

(3) *Image given to the data subject* [155]; and

---

[148] See e.g. D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 46.
[149] See e.g. Office of the Information Commissioner, "Data Protection Act, 1998 - Legal Guidance", Version 1, not dated, p. 16, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (last accessed 26 November 2010)
[150] See also S. Gutwirth, *Privacy and the information age*, *o.c.*, p. 97. See also *infra*; nr. 100.
[151] Opinion 1/2010, *l.c*, p. 26.
[152] *Id.*
[153] *Id.*
[154] Opinion 1/2010, *l.c.*, p. 28.

(4) *Expertise of the parties* (if the expertise of the service provider plays a predominant role in the processing, it may entail its qualification as data controller)[156].

D. Dynamic perspective

98. VARIABILITY OF CONTROL – The functional nature of the controller concept implies that the legal status of an actor may vary (1) over time and (2) across activities. The same actor may act as a "controller" for certain activities and as a "processor" for others. Likewise, the legal status of an actor might change from that of a "processor" to that of a "controller" (et vice versa) if there is a substantial change in its influence over the processing.[157] In each case, the qualification of an actor as either controller or processor has to be assessed with regard to specific sets of data or operations.[158]

99. OPERATION OR SET OF OPERATIONS – According to article 2(d), the influence of a controller extends to the "processing of personal data". Article 2(b) of the Directive defines the processing of personal data as "*any operation or set of operations which is performed upon personal data*". As result, the concept of a controller can be linked either to a single processing operation or to a set of operations. According to the Article 29 Working Party, the question of which entity is acting as a controller should be looked at "*both in detail and in its entirety*".[159] Specifically

> "*In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means.*"[160]

100. ASSESSMENT – The Working Party does not explicitly state when control should be assessed either at the level of a specific operation or set of operations. The examples provided suggest that the pursuit of a jointly defined purpose should be

---

[155] See Opinion 1/2010, *l.c.*, p. 28 (example of a call centre using the identity of the controller when communicating with data subjects).
[156] According to the Working Party, the traditional role and professional expertise of the service provider play a predominant role and may entail its qualification as data controller. See Opinion 1/2010, *l.c.*, p. 28-29 (describing the situation of barristers and accountants). See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 62 (noting that if the processing of personal data is a correlary of another service being provided, than the service provider is a controller rather than a processor).
[157] For example, if a processor suggests to the controller to use personal data for a new purpose and both parties determine how this processing shall be organized, the processor will likely be considered a controller with respect to these further processing activities.
[158] Opinion 1/2010, *l.c.*, p. 25.
[159] *Ibid*, p. 3 and 20-21.
[160] *Ibid*, p. 20.

determinative.[161] An alternative approach, advanced by the Dutch legislature, would be to again simply look at general perception. If the "prevailing norms of social interaction" treat a series of processing operations as a "cohesive whole", control should be assessed in relation to the set of operation rather than at the level of each individual operation.[162] Given the central importance of the purpose specification principle to the regulatory scheme of EU data protection law, however, the delineation of "the processing" should be made in light of the purposes pursued.[163] As Gutwirth argues:

> "*[T]he delineation and separation of purposes is decisive in the establishment of the number of processing operations. Finality is the key to pinpoint what the processing operation is. And since the whole protection system is engrafted onto the processing operation, it will succeed or fail based on the way in which processing is delineated. Personal data processing is each processing operation or series of operations with personal data which aims to realize one purpose, one finality.*"[164]

3 RELATIONSHIP BETWEEN (CO-)CONTROLLERS

101. OUTLINE – Article 2(d) recognises the possibility that more than one actor exercises control over the processing ("alone or jointly with others"). The relationship among two actors that determine the purposes and means of the processing *together* is referred to as a relationship of "joint control" or "co-control". Joint control should be clearly distinguished, however, from situations where multiple actors each determine their own purposes and means *independently* of one and other ("separate control").

3.1 "JOINT CONTROL" VS. "SEPARATE CONTROL"

A. Joint control

102. PRINCIPLE – In case of joint control, the actors involved jointly determine the purposes and means of the processing. During the preparatory works, the European Commission noted that

> "*for a single processing operation a number of parties may jointly determine the purpose and means of the processing to be carried out. It follows from this that, in such a case, each of the co-controllers must be considered as being constrained by*

[161] See also *infra*; nr. 466.
[162] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 51.
[163] Gutwirth, S., *Privacy and the information age*, *o.c.*, p. 97.
[164] *Id.*

the obligations imposed by the directive so as to protect the natural persons about whom the data are processed." [165]

According to the Article 29 Working Party, the Commission's opinion offered only a partial view of the different forms of joint control that may be possible:

"*The Commission opinion did not completely reflect the complexities in the current reality of data processing, since it focused only on the case where all the controllers equally determine and are equally responsible for a single processing operation. Instead, the reality shows that this is only one of the different kinds of 'pluralistic control' which may exist. In this perspective, "jointly" must be interpreted as meaning "together with" or "not alone" in different forms and combinations.*"[166]

103. DIFFERENT FORMS OF JOINT CONTROL – In case of joint control, the decision-making power of each co-controller may vary. For example, the co-controllers may be "on an equal footing" in terms of decision-making, or there might be a dominant party among them. In fact, an indeterminable number of variations are possible.[167] As the Working Party puts it

"*in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared. […] A broad variety of typologies for joint control should be considered […] in order to cater for the increasing complexity of current data processing reality.*"[168]

B. Separate control

104. PRINCIPLE – Multiple controllers can interact in the processing of personal data without being considered as "joint" or "co-controllers". If an exchange of data takes place between two parties without shared purposes and means, the exchange should be viewed only as a transfer between separate controllers.[169] For instance, if each controller processes personal data for its own distinct purposes, each is likely to be considered as a controller independently of the other.

105. RECITAL (47) – Article 2(d) does not explicitly recognise the possibility of "separate control". Clear support can be found, however, in recital (47) of the Directive, which concerns the provisioning of electronic transmission services:

---

[165] Commission of the European Communities, Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (95) 375 final-COD287, 18 July 1995, p. 3.
[166] Opinion 1/2010, *l.c.*, p. 18.
[167] *Ibid*, p. 18-19.
[168] *Ibid*, p. 19.
[169] *Id*.

> *"Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service*".

Recital (47) is important for two reasons. First, it signals that when the processing involves multiple operations and multiple actors, there can be more than one controller, for each of the different actions that occur. Secondly, it suggests that if one actor decides to entrust personal data to another actor, the former is probably acting as a controller with regards to the transmitted content.[170] The actor receiving the data might be acting as a processor, but it might also be acting as a controller. Recital (47) indicates that the latter is likely to be the case with respect to the processing of "additional personal data necessary for the operation of the service".[171]

C. Decisive factor

106. PRINCIPLE – The distinction between "joint" and "separate" control may be difficult to draw in practice. The decisive factor is whether or not the different parties jointly determine the purposes and means of the processing at issue.[172] If the parties do not pursue the *same objectives* ("purpose"), or do not rely upon the *same means* for achieving their respective objectives, their relationship is likely to be one of "separate controllers" rather than "joint controllers". Conversely, if the actors in question do determine the purposes and means of a set of processing operations together, they will be considered to act as "joint controllers" or "co-controllers".[173]

---

[170] See also B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 69

[171] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 59-60 for a discussion of the respective obligations of the provider of an electronic communication service and the sender of the message, e.g. regarding data accuracy ("*Wat betreft de juistheid van de gegevens beperkt zich deze verantwoordelijkheid tot de zorg te waarborgen dat de gegevens in overeenstemming zijn met de gegevens zoals deze zijn aangeleverd door degene die van deze dienst gebruik maakt*"). See also Opinion 1/2010, *l.c.*, p. 29 (example of a lost & found website).

[172] Opinion 1/2010, *l.c.*, p. 19 ("*joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller*").

[173] See also Opinion 1/2010, *l.c.*, p. 25. The distinction between joint and separate control was rendered more explicit in the 1984 UK Data Protection Act, which defined a data user as the person that "either alone or jointly or in common with other persons" controls the contents and use of the data (Section 1(5) of the 1984 Data Protection Act). As clarified by the Data Protection Registrar: "*The control does not need to be exclusive to one data user. Control may be shared with others. It may be shared jointly or in common. 'Jointly' covers the situation where control is exercised by acting together. Control 'in common" is where each*

3.2 THE TYPOLOGY OF OLSEN AND MAHLER

107. OUTLINE – In 2005, Olsen and Mahler developed a very interesting visualization and typology of the different types of relationships among (co-)controllers and processors.[174] The typology encompasses, for the most part, the different forms of collaboration subsequently outlined by the Article 29 Working Party in Opinion 1/2010. In the interest of brevity, the following sections will combine the typology developed by Olsen and Mahler with examples given by the Article 29 Working Party in Opinion 1/2010.[175]

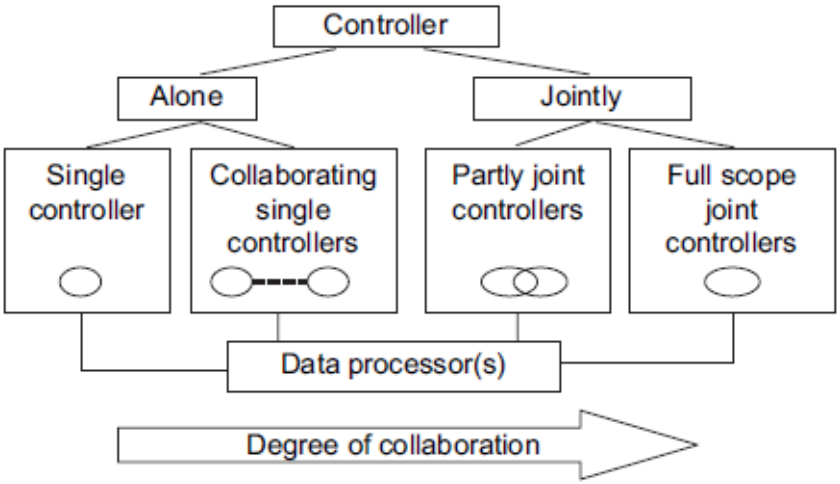

Figure 1: Modes of collaboration among (co-)controller(s) and processor(s)[176]
© T. Olsen and T. Mahler

A. *Single controller*

108. BASIC CHARACTERISTICS – The most straightforward scenario is that in which there is only one entity acting as a controller, without having any relationship

shares a pool of information, changing, adding to or using the information for his own purposes independently of the other". (The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Great Britain. Office of the Data Protection Registrar, Wilmslow, 1989p. 10-11.) See also the Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", Data Protection Registrar, Wilmslow, 1985, p. 12. Cf. *infra*; nr. 433.

[174] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *Legal IST project*, Deliverable D11, 4 November 2005, p. 40-47. The relevant parts of the Legal IST report were later published as T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 419-420.

[175] Due to the wide range of possible ways in which joint control might be exercised, the Article 29 Working Party decided not to develop a former typology of co-control. (See Opinion 1/2010, *l.c.*, p. 18). The examples it provided can, however, for the most part, be categorized within the Olsen-Mahler typology.

[176] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 419.

whatsoever with other data controllers.[177] This controller might be carrying out the processing by itself, or rely on the services of a processor. Insofar as the latter only acts pursuant to instructions provided by the former, there shall be little doubt as to which actor is legally responsible for ensuring compliance under data protection law.

B. Collaborating single controllers

109. BASIC CHARACTERISTICS – In this scenario, there is an interaction between data controllers, but they do not make any joint decisions about the purposes and means of any specific processing operation.[178] The "collaborating single controllers" do exchange personal data with one and other, but each party has its own reasons to process the data.[179] The relationship among collaborating single controllers has also been referred to by the Article 29 Working Party as a relationship among "separate controllers".[180]

110. EXAMPLE – A travel agency sends personal data of a customer to an airline and a chain of hotels in order to make reservations. Once the airline and hotel have confirmed the availability of the rooms requested, the travel agency issues the relevant tickets and vouchers. In such a scenario, the travel agency, the airline and the hotel are to be considered as three separate data controllers, each subject to the data protection obligations relating to its own processing of personal data.[181]

C. Partly joint controllers

111. BASIC CHARACTERISTICS – The third type of collaboration envisaged by Olsen and Mahler is the situation where the purposes and means of certain processing operations are determined jointly by more than one controller, while other processing operations are performed separately under the sole control of one controller.[182]

112. EXAMPLE – A typical scenario in which partial joint control arises is when several (otherwise autonomous) business entities decide to create a common web portal. For example, the travel agency, hotel chain and airline decide to create a common web portal to manage their respective reservations. They all agree on the means to be used (e.g., which data will be stored, who can have access, etc.) and the overall purpose for each actor is the same. Furthermore, they pool their customer information to carry out integrated marketing actions. In this scenario the travel agency, hotel and airline are to

---

[177] *Ibid*, p. 419.
[178] *Id*.
[179] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 44.
[180] Opinion 1/2010, *l.c.*, p. 19.
[181] *Id*. Recital (47) offers another example of "collaborating single controllers". Cf. *supra*; nr. 105.
[182] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 420.

be considered joint controllers for the processing operations which are accomplished on the jointly controlled portal, but as single controllers with regard to further processing carried outside of the portal.[183]

113. VARIATIONS – "Partial joint control" can be seen as a combination of "collaborating single control" (type *B*) and "full scope joint control" (type *D*). It should be reiterated, however, that the decision-making power of each joint controller may vary, whereby the actors involved determine the purposes and means to a different extent. In other words, the exercise of control may be "symmetric" or "asymmetric": (co)controllers may be "on an equal footing" in terms of decision-making, or there might be a dominant party among them.[184]

D. Full scope joint controllers

114. BASIC CHARACTERISTICS – Collaborating entities shall be considered to be acting as "full scope" (or "full-fledged"[185]) joint controllers when they jointly determine *all* the purposes and means of the data processing operations involved in a particular application or in the provisioning of a particular service.[186] In this scenario the collaborating entities shall in principle be jointly and equally responsible for compliance with all applicable data protection requirements.[187]

115. EXAMPLE – An example of full scope joint control might occur when two or more research institutions jointly process personal data as part of a common research project.[188]

3.3 CONTRACTUAL FLEXIBILITY

116. NO SPECIFIC PROVISIONS – In contrast to the relationship among controllers and processors, Directive 95/46/EC does not contain any requirements regulating the relationship among controllers as such.[189] While the Directive does not explicitly require

[183] Opinion 1/2010, *l.c.*, p. 20.
[184] See also Opinion 1/2010, *l.c.*, p. 22.
[185] *Ibid*, p. 21.
[186] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.*, p. 420.
[187] *Id.*
[188] *Id.*
[189] One notable exception has resulted from the administrative practice surrounding international transfers. Article 26 (2) has provided the basis for the use of contractual clauses as a means to enable transfers to jurisdictions not providing an "adequate" level of protection. Pursuant to the powers conferred by article 26 (4), the Commission has developed standard contractual clauses for transfers to both data controllers and data processors established outside the EU/EEA. See http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm. For more information on the regulation of transborder data flows see C. Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", *TILT Law & Technology Working Paper Series*,

controllers to conclude a contract with each other, the Working Party has stated that an agreement should be in place as to how compliance with data protection rules shall be ensured. Collaborating controllers are said to enjoy a degree of flexibility when allocating responsibility amongst each other, "as long as they ensure full compliance".[190] More specifically, the bottom line should be that:

> *"[…] even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties."*[191]

4 LIABILITY EXPOSURE OF CONTROLLERS AND PROCESSORS

117. OUTLINE – Directive 95/46/EC assigns the primary responsibility for compliance to the controller, as well as the corresponding liability exposure. Processors shall as a rule only be indirectly accountable for compliance with Directive 95/46/EC.[192] The distribution of responsibility and liability among controllers and processors results from a combination of provisions, which will be highlighted briefly over the following paragraphs. After that, this section will discuss different possible configurations, based on the typology presented above.

118. CONTROLLER – The allocation of responsibility upon the controller is first made explicit in article 6(2) of the Directive. This provision stipulates unambiguously that it shall be the controller who must ensure that the principles of data protection (as contained in article 6(1)) are complied with. In addition, the Directive specifies a wide range of additional obligations (accommodation of data subject rights, maintaining an appropriate level of security, etc.) which are incumbent upon the controller. Finally, article 23 of the Directive explicitly confirms that the liability for damages caused by non-compliant behaviour shall be borne by the controller, unless he can prove that he is not responsible for the event giving rise to the damage suffered.[193]

2010, 90p., available at http://www.tilburguniversity.edu/research/institutes-and-research-groups/tilt/publications/workingpapers/ckuner16.pdf (last accessed 1 August 2011).

[190] Opinion 1/2010, *l.c.*, p. 24.

[191] *Ibid*, p. 22.

[192] See also J. Alhadeff and B. Van Alsenoy (eds.), "D6.2 Contractual framework", Trusted Architecture for Securely Shared Services (TAS^3), second iteration, December 2009, p. 31, available at http://vds1628.sivit.org/tas3/content/deliverables/TAS3_D6p2_v2_TContractual_Framework.pdf (last accessed 1 August 2011)

[193] See also Opinion 1/2010, *l.c.*, p. 4.

119. PROCESSOR – As far as the processor's obligations are concerned, the Directive is far more succinct. In fact, the Directive articulates obligations addressed directly towards the processor only in one instance, namely in article 16. Article 16 provides that the processor may only process personal data pursuant to the instructions of the controller.[194] In addition, the processor shall in principle be obligated to observe all relevant aspects of data protection law by virtue of the contract which must be concluded among controllers and processors (article 17(3)).[195]

4.1 SINGLE CONTROLLER

120. LIABILITY FOR NON-COMPLIANCE – In case of a single controller, there shall in principle only be one actor responsible for compliance and thus liable in case of non-compliance. Article 23(1) provides that, as a general rule, the controller shall be liable towards data subjects for any damages suffered "*as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive*". Article 23(2) recognizes an exception, however, by stipulating that "*the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage*".

121. NATURE OF CONTROLLER OBLIGATIONS – Directive 95/46 imposes a variety of obligations upon controllers. In certain instances, these obligations specify a *result* to be achieved (e.g., "personal data must be collected for legitimate purposes and not further processed in a way incompatible with those purposes").[196] In other instances, the obligations of the controller are specified as an obligation to make reasonable efforts to do something ("*obligation of means*" or "*obligation des moyennes*"). For example, article 6(1)d provides that the controller must take "every reasonable step" to ensure that data which are inaccurate or incomplete shall be erased or rectified. Similarly, article 17(1) requires the controller to implement "appropriate" measures to ensure the security of processing. Finally, it should be noted that certain requirements necessitate further assessment in light of the specific circumstances of the processing (e.g., whether or not personal data are "excessive" will depend inter alia on the purposes of the processing). The precise nature of the controller's obligations must therefore be determined in light to the specific wording of each provision.

122. BURDEN OF PROOF – To hold a controller liable, a data subject must be able to demonstrate three elements, namely (1) the performance of an "unlawful act" (i.e. an unlawful processing operation or other act incompatible with the national provisions adopted pursuant to the Directive); (2) the existence of damages; and (3) a causal

[194] Cf. *supra*; nr. 78.
[195] See also Opinion 1/2010, *l.c.*, p. 26 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *Computer, Law & Security Review* 2007, Vol. 23, no 5, p. 418.
[196] Article 6(1)b Directive 95/46/EC.

relationship between the unlawful act and the damages incurred.[197] In addition, the data subject must also establish, as a preliminary matter, that the defendant is (or was) acting as the "controller" of the processing.[198]

123. ASSESSMENT – The burden of proof incumbent upon data subjects is quite onerous. First, identifying the controller of the processing may be a complicated exercise, especially where more than one party is involved in the processing. Second, demonstrating the performance of an "unlawful act" is also a challenge, particularly where the Directive does not specify an obligation of result or requires further interpretation (e.g., an assessment of proportionality).[199] Demonstrating causality can also be difficult, especially in cases where a particular outcome may be caused by different factors.[200] For example, it may be difficult to prove that the unlawful collection of information (e.g., information regarding the ethnicity of a loan applicant) actually caused the damages to occur (e.g., the denial of a loan may be attributed to many different factors).[201]

---

[197] D. De Bot, "Art. 15bis Wet Persoonsgegevens", in X., *Personen- en familierecht. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2001, looseleaf. See also Raad van State, Advies van de Raad van State bij het voorontwerp van wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij Verkeer van die gegevens, 2 February 1998, *Parl. St.* Kamer 1997-1998, nr. 1566/1, p. 145. See also U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 264.

[198] See also Study Group on a European Civil Code and the Research Group on EC Private Law, "Principles, Definitions and Model Rules of European Private Law - Draft Common Frame of Reference (DCFR)", 2009, p. 2994, paragraph 31, accessible at http://ec.europa.eu/justice/contract/files/european-private-law_en.pdf (last accessed 8 September 2015) ("*[…] as far as tort law is concerned, is that the plaintiff must plead/establish and prove all of the requirements pertaining to his claim, in particular damage, grounds of liability and causation save where express regulations permit departures from this rule, whereas it is incumbent upon the defendant to show and prove certain requirements which give rise to a ground of defence, thereby displacing the claimant's assertions*") (hereafter: "DCFR"). See also the Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161 and the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraph 141.

[199] T. Léonard and Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution", *l.c.*, p. 394, nr. 65 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", *l.c.*, looseleaf.

[200] In this regard, it is worth noting that the European Union Civil Service Tribunal has held that the burden of proof incumbent upon the applicant may be relaxed "*in cases where a harmful event may have been the result of a number of different causes and where the Community institution has adduced no evidence enabling it to be established to which of those causes the event was imputable, although it was best placed to provide evidence in that respect, so that the uncertainty which remains must be construed against it*" (Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43, paragraph 161). See also the Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254, paragraphs 141-142.

[201] T. Léonard and Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution", *l.c.*, p. 394, nr. 65 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", *l.c.*, looseleaf. De Bot indicates the doctrine of lost opportunity (in Dutch "*verlies van een kans*") might be useful in this respect: see D. De Bot, "Art. 15bis Wet Persoonsgegevens", *l.c.*, looseleaf. Regarding possible improvements to the implementation of burden of proof provisions in discrimination cases see L. Farkas and L. O'Farrell, "Reversing the burden of proof: Practical dilemma's at the European and national level", European Commission, Directorate-General for Justice and Consumers, 2015, p. 81 et seq., available at http://ec.europa.eu/justice/discrimination/files/burden_of_proof_en.pdf (last accessed 30 March 2016).

124. ELIGIBLE DAMAGES – In principle, there is no restriction as to the type or amount of damages that data subjects may claim. Data subjects can claim both material (e.g., loss of an opportunity) and non-material damages (e.g. loss of reputation, distress).[202] Of course, the general rules on damages shall also apply here (e.g. personal interest, actual loss, etc.).[203]

125. ESCAPE CLAUSE – Article 23(2) provides that the controller may be exempted from liability only if "*he proves that he is not responsible for the event giving rise to the damage*". The question inevitably arises as to the nature of the burden of proof incumbent upon controllers. Which evidence must controllers offer to successfully exempt themselves from liability, either for their own actions or for the actions performed by their auxiliaries?

126. LEGISLATIVE HISTORY – During the legislative history of Directive 95/46, the escape clause of article 23(2) underwent several revisions. In the initial Commission proposal, the escape clause provided that the controller of the file would not be liable for damages resulting from the *loss or destruction of data* or from *unauthorized access* if he could prove that he had taken "*appropriate measures*" to comply with requirements of articles 18 and 22 (security and due diligence).[204] The European Parliament amended the text to state that the controller must compensate the data subject for *any* damage "*resulting from storage of his personal data that is incompatible with this directive*."[205] The Parliament's change had the effect of removing the escape clause contained in the initial Commission proposal.[206] The European Commission felt strongly, however, that the Member States should be able to exempt controllers from liability, if only in part, for damage resulting from the loss or destruction of data or from unauthorized access "*if he*

---

[202] U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 263 and D. De Bot, "Art. 15bis Wet Persoonsgegevens", *l.c.*, looseleaf. See also Court of Appeal (Civil Division), *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311 (27 March 2015), at paragraphs 70-79, accessible at http://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html. It should be noted that the UK Supreme Court has granted permission to appeal this decision https://www.supremecourt.uk/news/permission-to-appeal-decisions-28-july-2015.html (last accessed 8 September 2015).

[203] For a discussion of the general rules of damages under Belgian law see e.g. S. Stijns, *Verbintenissenrecht*, Boek 1bis, Brugge, Die Keure, 2013, p. 101-104.

[204] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, SYN 287 and 288, 13 September 1990, p. 40.

[205] European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading) O.J. 13 April 1992, C 94/192.

[206] The change proposed by the Parliament should be neither overstated nor understated. In both versions, the controller only risks liability in case of failure to comply with the obligations imposed by the Directive. A key difference however, concerns the lack of reference to "due diligence requirement" of (former) article 22. By explicitly referring to (former) article 22, the initial Commission proposal implied that a controller might escape liability for a security breach if he could demonstrate having exercised appropriate care in choosing his processor. In the European Parliament version, however, it is clear that the controller would remain liable for ensuring compliance with the security obligation, even if the controller had exercised appropriate care in choosing his processor.

proves that he has taken suitable steps to satisfy the requirements of Articles 17 and 24."[207] In the end, the issue was settled by the Council, which drafted the final version of 23(2), which provides that:

> "*The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.*"

The Council clarified the meaning of article 23(2) by way of a recital which stipulated that

> *"[…] whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he reports an error on the part of the data subject or in a case of force majeure*".

127. DEFENCE – In order to prove that he is "not responsible for the event giving rise to the damage", the controller must demonstrate three things: (1) the occurrence of an event; (2) which caused the damage; and (3) which cannot be attributed to the controller.[208] In principle, mere demonstration of an absence of fault on the part of the controller will not be sufficient.[209] Once it is established that the damage was caused by an unlawful processing operation, the controller can only escape liability by demonstrating that the damages occurred only as the result of an event which cannot be attributed to him.[210] Recital (55) provides two examples: "*an error on the part of the data subject*"[211] or "*a case of force majeure*"[212]. According to the parliamentary works relating to the implementation of Directive 95/46 into Belgian law, other events which

---

[207] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, O.J. 27 November 1992, C 311/54. See also Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 33.

[208] This point was emphasized by the Belgian Council of State during its evaluation of the bill implementing Directive 95/46. See Raad van State, Advies van de Raad van State bij het voorontwerp van wet tot omzetting van de Richtlijn 95/46/EG, *l.c.*, p. 145.

[209] *Ibid*, p. 146.

[210] See in the same vein also M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *University of Hong Kong Faculty of Law Research Paper* No. 2015/45, p. 23-24, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2683301 (noting that the language of article 23(2) does not concern itself with the imputation of fault or culpability to the controller, but with the imputation of the facts themselves).

[211] The reference to "*an error on the part of the data subject*" recalls the concept of "*contributory negligence*" or "*contributory fault*", whereby a victim whose own faulty behaviour has contributed to the occurrence of his own damage, is not entitled to compensation to the extent that his behaviour contributed to the damage. See Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3475-3500 and p. 3539. See also H. Cousy and D. Droshout, "Fault under Belgian Law", in P. Widmer (ed.), *Unification of Tort Law: Fault*, 2005, Kluwer Law International, p. 36.

[212] "*Force majeure*" or "*Act of God*" can be described as an unforeseeable and unavoidable event which occurs independent of a person's will. For a discussion of the specific requirements for force majeure in different Member States see Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3540 et seq.

cannot be attributed to the controller can also be considered as a possible defence (e.g., the act of a third party for which the controller is not accountable).[213]

128. AN EVENT BEYOND CONTROL – The wording "*an event which cannot be attributed to him*" recalls the concept of an "*external cause*" (in Dutch: "*vreemde oorzaak*") or "*event beyond control*", which in many jurisdictions is accepted either (1) as a justification ground excluding fault or (2) as a means to demonstrate the absence of a causal relationship.[214] According to the Draft Common Frame of Reference for European Private Law, an event beyond control is "*an abnormal occurrence which cannot be averted by any reasonable measure*" and which does not constitute the realisation of a risk for which the person is strictly liable.[215]

129. A FORM OF STRICT LIABILITY? – The liability rule of article 23 has been characterized as a form of strict (i.e. "no fault") liability.[216] The reason for the characterization appears to be that a controller cannot escape liability by demonstrating the absence of a "personal fault", or that it is not necessary for data subjects to demonstrate that the unlawful act was personally committed by the controller.[217] In my view, the characterisation of controller liability as strict liability can be deceiving.[218] Even though the data subject is not required to demonstrate a "personal fault" on the part of the controller, he must still succeed in proving the performance of an "unlawful act".[219] Demonstration of an "unlawful act" in principle amounts to a demonstration of

---

[213] Memorie van Toelichting bij het Wetsontwerp tot omzetting van de Richtlijn 95/46/EG, *l.c.*, p. 54 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 241. Of course, the presence of a justification ground does not suspend the general duties of care of a controller. If the controller could have foreseen the damages and prevent them by taking anticipatory measures, normal rules of negligence apply. See also Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3538 and H. Cousy and D. Droshout, "Fault under Belgian Law", *l.c.*, p. 43.

[214] See Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3538 et seq.

[215] *Id*. See also Article 7:102 of the Principles of European Tort Law (PETL). For a more detailed description of the situation under Belgian law see H. Cousy and D. Droshout, "Fault under Belgian Law", *l.c.*, p. 44 and S. Stijns, *Verbintenissenrecht*, *o.c.*, p. 58 et seq.

[216] Memorie van Toelichting bij het Wetsontwerp tot omzetting van de Richtlijn 95/46/EG, *l.c.*, p. 54 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 241 See also T. Léonard en Y. Poullet, "La protection des données à caractère personnel en pleine (r)évolution", *l.c.*, p. 394, nr. 65. Certain authors refer to the "objective liability" (in Dutch: "*objectieve aansprakelijkheid*") of the controller. Although these terms appear to be used interchangeably by many authors, some authors associate different legal consequences to the respective terms. For purposes of conceptual clarity, only the term "strict liability" shall be used here. For a discussion of the use of these terms see Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 2992 et seq. See also H. Cousy and D. Droshout, "Belgium", in B.A. Koch and H. Koziol (ed.), *Unification of Tort Law: Strict Liability*, 2002, Kluwer International, p. 43.

[217] Memorie van Toelichting bij het Wetsontwerp tot omzetting van de Richtlijn 95/46/EG, *l.c.*, p. 54 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 241.

[218] See also E. Reid, "Liability for Dangerous Activities: A Comparative Analysis", *The International and Comparative Law Quarterly* 1999, Vol. 48, No. 4, p. 736-737 (noting that strict liability is not always "stricter "than fault-based liability, particularly in cases where the circumstances giving rise to liability coincide in large measures with those used in negligence analysis).

[219] Cf. *supra*; nr. 122. See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 176. See also

"fault" for tort law purposes.[220] Conversely, if the controller can establish that the processing complies with the requirements of the Directive, he will effectively exempt himself from liability on data protection grounds.[221] The characterization of controllers liability as "strict liability" (i.e. the notion that a controller may be still be held liable in absence of a personal fault) is mainly relevant in relation to (1) controller obligations which impose an obligation of result; (2) the vicarious liability of a controller for acts committed by his auxiliaries or (3) the liability of a controller for acts committed by his processor (cf. *infra*; nrs. 132 et seq).

130. CONTRACTUAL VS. NON-CONTRACTUAL LIABILITY – The liability of the controller is in principle non-contractual in nature. The "fault" giving rise to liability is a breach of the law rather than the breach of a contractual agreement. As a result, it is by no means required that there exists a contractual relationship between the data subject and the controller. In cases where a contractual agreement exists, however, the unlawful processing operation may additionally constitute a violation of a contractual agreement. The rules governing a plaintiff's ability to combine contractual and non-contractual liability claims (concurrence of claims) may vary from Member State to Member State.[222]

4.2 CONTROLLER-PROCESSOR RELATIONSHIP

131. BASIC PRINCIPLE – Directive 95/46/EC bestows upon the controller the duty to ensure compliance. Because the processor is seen as a "mere executor", who merely acts in accordance with the instructions issued by the controller, the Directive maintains that the responsibility for ensuring compliance remains with the controller. Provided that the processor merely executes the instructions bestowed upon him, the consequences of its actions shall in principle be attributed to the controller rather than the processor.

P. Larouche, M. Peitz and N. Purtova, *Consumer privacy in network industries – A CERRE Policy Report*, Centre on Regulation in Europe, 25 January 2016, p. 58, available at http://cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf (last accessed 25 March 2016) (""*[A]t the end of the day, the DPD [...] create[s] little more than a basic fault-based regime for privacy and data protection breaches, with a reversed burden of proof.*")

[220] See article 4:101 and 4:102(3) of the Principles of European Tort law (PETL): "*A person is liable on the basis of fault for intentional or negligent violation of the required standard of conduct*" and "*Rules which prescribe or forbid certain conduct have to be considered when establishing the required standard of conduct.*") See also H. Cousy and D. Droshout, "Fault under Belgian Law", *l.c.*, p. 32.

[221] See also Kh. Kortrijk, 1ste Kamer, 19 June 2003, *T.G.R.* 2007, p. 96 ("*To the extent that the use of personal data complies with the data protection act, it cannot consitute a "fault" as such within the meaning of article 1382 Civil Code*"). This judgment was confirmed upon appeal: see Gent, 6 January 2005, *T.G.R.* 2007, p. 92.

[222] See e.g. Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3023-3028. In Belgium, there are certain limits as to the extent a plaintiff can invoke extra-contractual liability against a contracting party (in Dutch this is referred to as: "*samenloop*"). See e.g. S. Stijns, *Verbintenissenrecht*, *o.c.*, p. 128-142 and H. Bocken, "Samenloop contractuele en buitencontractuele aansprakelijkheid", *NjW* 2007, nr. 169, p. 722-731. In cases where the tort ("fault") giving rise to liability also amounts to a crime (which may often be the case where unlawful data processing is involved), the plaintiff in principle is not restricted from invoking extra-contractual liability (see S. Stijns, *o.c.,* p 125-128). The distinction between contractual and extra-contracutal liability is relevant inter alia for the determination of eligible damages (see H. Cousy and D. Droshout, "Belgium", *l.c.*, p. 61.)

132. NON-DELEGABLE DUTY OF CARE – Article 23(1) provides that, as a general rule, the controller shall be liable towards data subjects for any damages suffered as a result of non-compliance. The mere fact that the unlawful action was performed by the processor rather than the controller will not diminish the controller's liability exposure.[223] The controller shall in principle be liable for any violations of the Directive resulting from the operations carried out by a processor acting on its behalf ("*as if they were performed by the controller*"). In other words, the Directive 95/46 imposes upon controllers a "non-delegable duty of care": the duty of care which a controller owes data subjects cannot be transferred to an independent contractor.[224]

133. NO DUE DILIGENCE DEFENCE – A controller cannot escape liability for actions undertaken by its processors by demonstrating an absence of fault in either his choice or supervision of the processor.[225] This is a consequence of the "strict" liability imposed upon controllers: a controller can only escape liability by demonstrating that the processing complies with the requirements of the Directive or by proving an "*event beyond his control*" (article 23(2)).[226] The EU legislator deliberately chose to attach liability to the quality of a person as data controller (*qualitate qua*), without making any reference to possible exemptions other than the one mentioned in article 23(2).[227]

134. SIMILAR TO LIABILITY FOR AUXILIARIES – The liability of the controller for the actions performed by its processor is similar to the vicarious liability[228] of a principal for the actions undertaken by his auxiliaries, whereby "*a person is liable for damage caused by his auxiliaries acting within the scope of their functions provided that they violated the required standard of conduct*".[229] In case of processors, however, the

---

[223] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 176.

[224] Compare E. Reid, "Liability for Dangerous Activities: A Comparative Analysis", *l.c.*, p. 752-753 (explaining that a principal may be liable for the negligence of its contractors in cases where the law imposes a non-delegable duty of care). Liability for breach of non-delegable duty of care is not the same as vicarious liability, although the two can easily be confused. In case of vicarious liability, liability is "substitutional", whereas in case of a non-delegable duty of care, liability is personal (i.e. originates from a duty which is personal to the defendant). For a more detailed discussion see C. Witting, "Breach of the non-delegable duty: defending limited strict liability in tort", *University of New South Wales Law Journal* 2006, Vol. 29, No. 3, p. 33-60, accessible at http://www.austlii.edu.au/au/journals/UNSWLJ/2006/38.html (last accessed 18 April 2016).

[225] Contra: U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 264 (arguing that the intent of the European legislator was to exempt the controller not only in case of force majeure but also in cases where the controller had taken all the appropriate measures required by article 17).

[226] Cf. *supra*; nr. 128.

[227] The legislative history of 23(2) makes clear that the EU legislator intended to render the controller strictly liable for the actions committed by his processor by removing the reference to "suitable measures" (which had been present in both the initial and amended European Commission proposal) and by limiting the possible defense of the controller to "events beyond his control", such as force majeure. Cf. *supra*; nr. 126 and compare Art. 7:102 of the Principles of European Tort Law (PETL) (defences against strict liability). It stands to reason that the EU legislator thus deliberately chose to derogate from the general principle that a person shall not be liable for the actions performed by independent contractors.

[228] In Dutch: "*kwalitiatieve aansprakelijkheid*"; in French "*responsabilité du fait d'autrui*".

[229] Art. 6:102 of the Principles of European Tort Law (PETL). See also Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3318 et seq. In Belgium, the liability of a

relationship with the controller in principle is not hierarchical in nature. While the processor is legally prohibited from processing the data "except on the instructions of the controller", he is not necessarily a "subordinate" of the controller.[230] As a result, the processor will in principle not be formally considered as an "auxiliary" of the controller for tort law purposes, although the final outcome may be similar in practice.[231]

135. RATIO LEGIS – The preparatory works make clear that the liability of a controller for the activities of its processor stems from the fact that the controller is the person or body who "ultimately" decides about the design and operation of the processing carried out. A processor, on the other hand, is seen as someone who merely carries out the controller's instructions.[232] The preparatory works are silent as to why the decision was made to impose *strict* liability upon the controller. It stands to reason that the decision was the result of a compromise between the position of the European Commission (which favoured a more lenient approach) and that of the European Parliament (who favoured an even stricter approach).[233] Possible motivations for the imposition of a strict liability regime include: (1) the risks presented by the processing of personal data; (2) the wish to stimulate highly diligent behaviour on the part of the controller; or (3)

---

principal for the actions of his auxiliaries was historically rooted in a presumption of fault on the part of the principal, either in his choice of auxiliaries ("*culpa in eligendo*"), or in the exercise of supervision on the activities of the auxiliary ("*culpa in vigilando*"). Today, the liability of the principal for the actions of his auxiliaries is viewed as a legal safeguard designed to ensure the availability of an adequate remedy for aggrieved individuals. As a result, the principal is not allowed to provide evidence to refute the presumption of his fault as a defence (e.g., by demonstrating he made no fault either in the choice of supervision of his auxiliaries). (H. Vandenberghe, "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, afl. 2, p. 611.) See also H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", in J. Spier (Ed.), *Unification of Tort Law: Liability for Damage Caused by Others*, Kluwer Law International, London, 2003, p. 38-39.

[230] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 61. For a relationship of subordination to exist, the principal must enjoy the legal authority to issue instructions and to supervise the execution of tasks bestowed upon the auxiliary: see T. Vansweevelt en Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, Antwerpen Intersentia, 2009, p. 400; E. Dirix, "Aansprakelijkheid van en voor hulppersonen", in. M. Storme (ed.), *Recht Halen uit Aansprakelijkheid*, Gent, Mys & Breesch, 1993, p. 342-346; H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", *l.c.*, p. 46-50. While article 17(2) Directive suggests that the controller must "supervise "the processor's implementation of organisational and security measures (by using the phrasing "and must ensure compliance with those measures") (cf. *supra*; nr. 82), the Directive does not bestow upon the controller a general power of instruction or supervision. On the other hand, one could also argue that the reference to "authority" in article 16 of the Directive implies that the processor should be viewed as an "auxiliary" in relation to the processing activities carried out on behalf of a controller.

[231] Needless to say, in cases where the processor is a natural person, it may not be excluded that he or she might *de facto* operates in a hierarchical relationship with the controller, despite being labelled as an "independent contractor" in his or her contract with the employer. In cases where the person carrying out the services should legally be qualified as an "employee" rather than an "independent contractor", he or she will of course be treated as an "auxiliary" for tort law purposes.

[232] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 10.

[233] Cf. *infra*; nr. 490 et seq.

the wish to ensure the compensation of data subjects that suffer harm as result of the unlawful processing activities.[234]

136. DISREGARD FOR INSTRUCTIONS – Article 16 of Directive 95/46 requires the processor not to process personal data "*except on the instructions from the controller*". The question may therefore arise whether a controller shall remain liable for the activities of its processor when the processor disregards the controller's instructions. In this regard, a distinction might be made between two scenarios. In the first scenario (scenario A), the processor merely *fails to give effect* to the instructions issued by the controller (e.g., fails to implement the security measures instructed by the controller or fails to update information as instructed by the controller). In the second scenario (scenario B), the processor decides to process personal data *for his own purpose(s), beyond* the instructions received by the controller (in other words: to act outside the scope of his "processing mandate").

137. SCENARIO A – In scenario A, it is clear that the controller remains liable for the actions of its processor. The data subject should be compensated by the controller in full for all damages suffered as a result of the processor's actions. Article 23 of Directive 95/46 does not provide data subjects with a right to seek compensation from the processor. As a result, a data subject shall only be able to hold the processor liable on the basis of data protection legislation if this is provided by national law.[235] The Belgian Data Protection Act does not recognize a right for data subjects to hold processors liable as such. A data subject might still, however, be able to hold a processor liable if he can demonstrate that the actions of the processor constituted negligence or violated a legal provision.[236] It is in principle not excluded that the standard of care incumbent upon the processor be informed by the contract between controller and processor.[237] In any

---

[234] Based on H. Cousy and D. Droshout, "Belgium", *l.c.*, p. 62, who further note that strict liability regimes are typically justified by an amalgam of motives.

[235] See also Opinion 1/2010, *l.c.*, p. 28. ("*[W]hile the Directive imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, also the processor should be considered liable in certain cases*.") Article 49(3) of the Dutch Data Protection Act (Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) provides the processor can be held liable by data subjects insofar as the damages resulted his activities. See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, 62 and 176. Another example of a national law which imposes liability directly upon processors is the Czech Data Protection Act (see article 8 of Act No. 101/2000 Coll., on the Protection of Personal Data, 4 April 2000, English version accessible at https://www.uoou.cz/en).

[236] D. De Bot, "Art. 15bis Wet Persoonsgegevens", *l.c.*, looseleaf. Generally speaking, it will generally be more appealing for data subject to go after controller, because (a) the identity of the processor may not be known to the data subject (b) it will generally be more difficult for data subject to establish a violation of general duty of care by processor.

[237] See e.g. A. De Boeck, "Aansprakelijkheid voor gebrekkige dienstverlening", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Kluwer, 2008, II.3-84o-p. See also S. Demeyere, I. Samoy and S. Stijns, *Aansprakelijkheid van een contractant jegens derden – De rechtspositie van de nauw betrokken derde*, Brugge Die Keure, 2015, p. 37 et seq. The standard of care incumbent upon processor may in principle also be assessed in light of the professional occupation and knowledge of the processor: see e.g. H. Cousy and D. Droshout, "Fault under Belgian Law", *l.c.*, p. 32 and p. 39. In Belgium, plaintiffs may also

event, the controller should be able to obtain redress from the processor for disregarding his instructions on the basis of the contract between them.[238]

138. SCENARIO B – In scenario B, the processor does not merely fail to observe the instructions issued by the controller, but also decides to process the personal data for his own purposes. In such instances, the processor shall be considered to be acting as a controller in his own right, by virtue of determining his own "purposes and means" of the processing.[239] In such cases, the (former) processor can be held liable on the basis of national legislation implementing article 23 of Directive 95/46.[240] In principle, data subjects may also turn to the initial controller (who had entrusted the data to the processor) for compensation. This is a result of the strict liability regime of article 23. The initial controller cannot escape liability by demonstrating an absence of fault in either his choice or supervision of the processor.[241] In practice, this means that the data subject will in principle have the choice whether or not to sue both parties and whether or not to do so simultaneously or consecutively (although national tort law may specify otherwise).[242] The initial controller should be able to obtain redress from the processor for disregarding his instructions on the basis of the contract between them.[243] In the end, the outcome is that the (initial) controller will be forced to carry the risk of

---

need to consider the so-called "*rule of the (quasi-)immunity of the contractor's agent*" in cases where there is a contractual relationship between the controller and the data subject. This rule may further limit the data subject's ability to seek redress directly from the processor. If the action by the processor amounts to a crime, however, such limitations will not apply. For more information see H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", *l.c.*, p. 50; S. Stijns, *Verbintenissenrecht*, *o.c.*, p. 143 et seq. and I. Claeys, "Buitencontractuele aansprakelijkheid van contractanten en hulppersonen? Als het contractuele evenwicht maar niet wordt verstoord", in S. Stijns (ed.), *Verbintenissenrecht*, Die Keure, Brugge, 2004, Reeks 'Themis', nr. 23, p. 27-42. If both processor and controller can be held liable by the data subject, their liability will in principle be *in solidum*, which means that the data subject shall in principle have the choice whether or not to sue both and whether or not to do so simultaneously or consecutively. See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", in. W.V.H. Rogers (Ed.), *Unification of Tort Law: Multiple Tortfeasors*, Kluwer Law International, 2004, p. 34-35.

[238] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 176.

[239] See also Opinion 1/2010, *l.c.*, 25. A (former) processor shall be (re)qualified as a (co-)controller where he acquires a relevant role in determining either the purpose(s) and/or the essential means of the processing (*Id.*). See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 62.

[240] In principle, the processor may also be held liable on the basis of the national provision implementing article 16 of Directive 95/46, which specifies that the processor may not process personal data "*except on the instructions of the controller*", which is a requirement directly applicable to processors. Depending on the jurisdiction, a breach of confidentiality by processors may also amount to a crime: see e.g. article 38 of the Belgian Data Protection Act.

[241] Cf. *supra*; nr. 133. This outcome is similar to the liability of principals for torts committed by their auxiliaries "*in the course of the service*" for which they have been enlisted (although results may vary depending on national tort law). See e.g. T. Vansweevelt en Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, *o.c.*, p. 416-421 and H. Vandenberghe, "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, afl. 2, p. 604-606.

[242] In Belgium, victims of concurrent faults may hold both the tortfeasor and the vicariously liable party liable *in solidum*. See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 33-35 and H. Cousy and D. Droshout, "Belgium", *l.c.*, p. 68-69.

[243] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 176.

insolvency of his processors (in cases where his liability exposure stems from the processor's disregard of instructions).

4.3 COLLABORATING SINGLE CONTROLLERS

139. BASIC PRINCIPLE – Collaborating single controllers exchange personal data with one and other, but do so without making any joint decisions about the purposes and means of any specific processing operation.[244] In such cases, each party is independently (yet fully) responsible for ensuring compliance of its own processing activities. In principle, the liability exposure of each party is also strictly limited to the processing activities under its own control. In exceptional cases, however, liability may nevertheless be shared, particularly where a failure to ensure compliance by one controller contributes to the same damages caused by the fault by another controller.

140. SEPARTE CONTROL, SEPARATE RESPONSIBILITIES – In principle, collaborating single controllers are only responsible for ensuring compliance of their own processing activities. As Olsen and Mahler put it:

> "*In this type of multiple data controller relationship, the data controllers separately process personal data, but there is a data flow from one controller to the other. Each controller is responsible for his own processing, and the communication of personal data to the other data controllers is one example of such processing. One controller is not responsible for acts or omissions of the other data controller.*"[245]

Because each controller is separately responsible for his own processing activities, only one controller shall in principle be liable in case of an unlawful processing operation (scenario A).[246] Liability may nevertheless be shared, however, if the fault of one controller brings about the *same damage* as the fault of another controller (scenario B).

141. SCENARIO A – Hospital A maintains medical records of patient B. Hospital A routinely shares information about patient B's treatments with insurance company C, in order to obtain payment for the expenses relating to patient B's care. One day, insurance company C suffers a data breach as a result of insufficient security measures. Information about patient B's medical treatment is exposed, leading to considerable emotional harm. In principle, patient B will only be able to obtain compensation from insurance company C for the damages suffered because hospital A is not the controller of the processing operations undertaken by insurance company C.

---

[244] Cf. *supra*; nr. 109.
[245] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 41.
[246] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58.

142. SCENARIO B – Hospital A holds medical information on Patient B. One day, hospital A mistakenly transmits information about patient B's treatment to the wrong insurance company, namely insurance company D. The next day, insurance company D suffers a data breach as a result of inadequate security measures. In such cases, patient B may be able to obtain compensation from both Hospital A and insurance company D for the damages suffered, as they each committed a fault contributing to the same damage.

143. CONCURRING FAULTS – Scenario B offers an example of *concurring faults* (in Dutch: "*samenlopende fouten*"), whereby several distinct faults may be considered to have caused the same legally relevant damage.[247] What precisely constitutes "*the same damage*" is open to interpretation.[248] In certain jurisdictions, concurring faults lead either to solidary liability or liability *in solidum*.[249] If that is the case, each "concurrent tortfeasor" shall be obliged to indemnify the victim for the entire damage, irrespective of the severity of the fault leading to its liability.[250] The internal allocation of liability between the concurrent tortfeasors may nevertheless take into account the extent or severity of the fault.[251] In the case of scenario B, it would mean that hospital A would be obliged to indemnify patient B for the whole of the damages suffered, even though hospital A was not responsible as a controller for the poor security measures employed by insurance company D. In principle, hospital A should be able to exercise redress against insurance company D for its contribution the damages.

4.4 JOINT CONTROL

144. BASIC PRINCIPLE – In case of joint control, several parties jointly determine the purposes and means of one or more processing activities.[252] Directive 95/46 EC is essentially silent on how responsibility and liability should be allocated in this scenario. The only guidance that can be found in the legislative history of Directive 95/46 is the following statement made by the European Commission:

---

[247] See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 29-35; S. Stijns, *Verbintenissenrecht*, *o.c.*, p. 110-111 and T. Vansweevelt en Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, *o.c.*, p. 835-839.

[248] *Ibid*, p. 44-45 and S. Guiliams, "Eenzelfde schade of andere schade bij pluraliteit van aansprakelijken", *Nieuw Juridisch Weekblad* (NJW) 2010, afl. 230, 699-700 (arguing that different faults will be considered to have contributed to "the same damage" *if it is practically impossible to distinguish* to what extent the damage is attributable to each of the concurring faults).

[249] See Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3599 et seq. See also art. 9:101 of the Principles of European Tort Law (PETL).

[250] *Id.* The difference between solidary liability and *in solidum* liability is minimal: in both cases, the injured party is able to sue each of the debtors for relief of the whole amount. For more information see H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 29-36 and See also H. Cousy and D. Droshout, "Belgium", *l.c.*, p. 68-69.

[251] *Id.* In Belgium, the apportionment of liability among the concurrent tortfeasors must in principle be based on the extent to which each concurring fault may be said to have caused the damage, rather than the severity of the fault. (S. Stijns, *Verbintenissenrecht*, *o.c.*, 2013, p. 111 and S. Guiliams, "De verdeling van de schadelast bij samenloop van een opzettelijke en een onopzettelijke fout", *Rechtskundig Weekblad* (R.W.) 2010-2011, nr. 12, p. 475).

[252] Cf. *supra*; nr. 114.

"each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed".[253]

145. SHARED CONTROL, SHARED RESPONSIBILITIES – In case of joint control, each controller is individually responsible for ensuring compliance of the processing as a whole. As a result, each joint controller shall in principle be liable for any damages resulting from non-compliance. The liability among joint controllers shall in principle be solidary in nature (i.e. the harmed data subject may bring a claim against any of them for the full amount).[254] Of course, the solidary liability of joint controllers only extends to those processing activities for which they in fact exercise joint control. In case of "partial joint control" (whereby certain processing operations are performed under the sole control of one controller)[255], responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.[256]

146. COMMON FAULTS – The solidary liability of joint controllers can be justified on the basis of the "common fault" committed by each controller. A "common fault"[257] arises when multiple parties knowingly and willingly contribute to the same circumstance or event giving rise to the damage.[258] A common fault in principle leads to solidary liability.[259]

147. BENEFITS – Solidary liability provides victims with a number of advantages. First, the risk of insolvency of one of the tortfeasors is shifted from the victim to the other tortfeasors.[260] In addition, the victim escapes the burden of specifying to which extent each tortfeasor has contributed to the damage.[261] As noted by the DCFR,

"*[t]he victim should not be expected to establish the respective shares of liability; this issue must be ironed out by the liable persons between themselves. It would be*

---

[253] Commission of the European Communities, Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (95) 375 final-COD287, 18 July 1995, p. 3 See also Opinion 1/2010, *l.c.*, p. 17-18.

[254] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 46-48. See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58.

[255] Cf. *supra*; nr. 111.

[256] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 46-48

[257] In Dutch: "*gemeenschappelijke fout*"; in French: "*faute commune*".

[258] See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 30; T. Vansweevelt en Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, *o.c.*, p. 839.

[259] *Id.* See also Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3599 et seq. See also art. 9:101 of the Principles of European Tort Law (PETL).

[260] H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 32.

[261] *Id.* See also Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3599.

unfair to require the injured person always to sue each and every liable person and dispute with them all and it would be especially unfair to require the injured person to bear the risk of personal insolvency of one of the liable persons. The injured person should in fact have the option of pursuing the person from whom reparation can probably be obtained most quickly and most easily."[262]

148. RECOURSE – If the data subject decides to address only one of the joint controllers for the damages, that controller should be able to obtain redress from his fellow joint controllers for their contribution to the damages.[263] In principle, nothing prevents joint controllers from deciding how to allocate responsibility and liability among each other (e.g., by way of a joint controller contract).[264] The terms of such arrangements should not, however, be opposable to data subjects, based on the principle of solidary liability for common faults.[265]

149. THE APPROACH OF WP29 – The Article 29 Working Party has argued that joint control should not necessarily entail solidary ("joint and several") liability.[266] According to the Working Party, "*in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared*".[267] Against this background, the Working Party argues that co-controllers should enjoy a certain flexibility when allocating responsibilities among each other "*as long as they ensure full compliance*".[268] As a result, the Working Party concludes that "joint control" should not necessarily entail solidary ("joint and several") liability.[269] Instead, joint and several liability

"should only be considered as a means of eliminating uncertainties, and therefore assumed only insofar as an alternative, clear and equally effective allocation of

---

[262] *Id.*

[263] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58.

[264] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 48.

[265] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58 ("*Bij gezamenlijke verantwoordelijkheid zijn alle in het samenwerkingsverband participerende personen c.q. instellingen hoofdelijk aansprakelijk. Uit de artikelen 6:6 e.v. BW vloeit voort dat iedere verantwoordelijke tegenover de betrokkene voor het geheel aansprakelijk is. Dit laat onverlet de mogelijkheid van regres wanneer bij voorbeeld de schuld bij één van de andere verantwoordelijken ligt.*")

[266] Opinion 1/2010, *l.c.*, 22. In this context, the term "solidary liability" is synonymous with the term "joint and several liability".

[267] *Ibid*, p. 21. See also *supra*; nr. 102.

[268] Opinion 1/2010, *l.c.*, 24. See also *supra*; nr. 102. According to the Working Party, the Commission only envisaged a situation where all controllers equally determine the purposes and means of the processing. This is, however, only one of several kinds of "pluralistic control", and responsibilities should allocated accordingly. See Opinion 1/2010, *l.c.*, p. 18-19.

[269] Opinion 1/2010, *l.c.*, p. 22.

obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances".[270]

In other words, the Working Party considers that joint controllers enjoy quite some "margin for appreciation" as far as the determination of responsibility and liability is concerned. One controller might be held responsible for certain aspects of the processing, while another controller might be responsible for others. In the end, it appears to be simply a matter of appreciation of the factual circumstances at issue.

150. ASSESSMENT – The approach of the Article 29 Working Party seems fair when it comes to the internal allocation of liability among joint controllers, but may potentially be unfair towards the harmed data subject. The Working Party's approach suggests that a contract between joint controllers may be opposable to data subjects, and that a harmed data subject may carry the burden of deciding which of the joint controllers is "ultimately" responsible for the damages suffered. In my view, the approach of the Working Party does not find sufficient support in either the text or legislative history of Directive 95/46/EC. In cases where joint control exists, each joint controller should incur solidary liability for damages resulting from the "common" processing. Any arrangements between joint controllers, including those regarding liability, should not be opposable to data subjects, based on the principle of solidary liability for common faults.[271]

5 SPECIFIC ISSUES

5.1 INDIVIDUALS WITHIN ORGANISATIONS

151. PROBLEM STATEMENT – Article 2(d) defines a controller as being a "*natural person, legal person, public authority, agency or any other body*". The definition thus refers to a broad range of subjects, ranging from natural to legal persons and including "any other body".[272] In practice, the question may arise whether an individual within an organisation should be considered as the "controller", or whether instead this role should attributed to the organisation of which he or she is a part. According to the Article 29 Working Party,

> "*preference should be given to consider as controller the company or body as such rather than a specific person within the company or the body. It is the company or the body which shall be considered ultimately responsible for data processing and the obligations stemming from data protection legislation, unless there are clear*

[270] *Ibid*, p. 24.
[271] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58. Again: in cases of partial joint control, responsibility and liability will only be shared with regard to the common (i.e. jointly controlled) processing activities.
[272] Opinion 1/2010, *l.c.*, p. 15.

elements indicating that a natural person shall be responsible. In general, it should be assumed that a company or public body is responsible as such for the processing activities taking place within its realm of activities and risks."[273]

152. RELATIONSHIP WITH OTHER AREAS OF LAW – In Opinion 1/2010, the Working Party emphasizes that it is important to stick as closely as possible to the rules established by other areas of law, such as civil, administrative and criminal law.[274] These rules indicate to what extent individuals, organisations or other bodies may be held responsible and will in principle help to determine which actor should be labelled as the "controller".[275] The following paragraphs will briefly look at the civil and criminal liability of organisations - and the individuals working on their behalf - from the perspective of Belgian law.

153. LIABILITY FOR AUXILIARIES AND AGENTS – Article 1384, subsection 3 of the Belgian Civil Code (C.C.) provides that masters and principals are liable for damage caused by their servants and appointees ("auxiliaries"). For article 1384, subs. 3 to apply, the following three conditions must be met:

a) there must be a relationship of *subordination* between the principal and the auxiliary;

b) the auxiliary must have committed a *fault* (i.e. negligence or unlawful act)

c) the fault must have been committed *in the course of the service* for which the auxiliary has been enlisted. [276]

Article 1384, subs. 3 C.C. is generally applied to hold employers (and legal persons more generally) vicariously liable for actions of their employees and other subordinates.[277] Public servants and directors of private corporations, on the other hand, are generally viewed as "organs", whose tortious behaviour can be imputed directly to the State or legal person on the basis of the theory of organic representation.[278]

---

[273] *Id.*

[274] *Id.* ("*The identification of 'the controller' in a data protection perspective will be interconnected in practice with the civil, administrative or criminal law rules providing for the allocation of responsibilities or sanctions to which a legal or a natural person can be subject.*") (*Ibid*, p. 16.)

[275] *Ibid*, p. 15. See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 387.

[276] See H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", *l.c.*, p. 46; H. Vandenberghe, "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, afl. 2, p. 596 et seq. and T. Vansweevelt and Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, *o.c.*, 399 et seq. See also Study Group on a European Civil Code and the Research Group on EC Private Law, "DCFR", *l.c.*, p. 3318 et seq. and art. 6:102 of the Principles of European Tort Law (PETL).

[277] Under Belgian law, the requirements concerning the vicarious liability of employers are interpreted quite broadly. For example, an act shall be considered to have been committed "*in the course of the service*" as soon as there exists some (even indirect) connection between the tort and the service for which the person has been enlisted. For more information see T. Vansweevelt and Britt Weyts, *Handboek Buitencontractueel Aansprakelijkheidsrecht*, *o.c.*, p. 418 et seq.

[278] H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", *l.c.*, p. 42 and B. Samyn, "Raad van Bestuur", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, II.1-26a et seq.

154. EMPLOYEE LIABILITY – In principle, any processing of personal data by employees which takes place within the "realm of activities" of an organisation may be presumed to take place under that organisation's control.[279] Employees are generally not considered as "controllers", but rather as "persons acting under the authority of the controller" within the meaning of article 16 of Directive 95/46. Nevertheless, employees may be subject to criminal or civil liability on the basis of national legislation implementing Directive 95/46. Recital (55) *in fine* of Directive 95/46 provides that "*[…] sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive*".[280] It should be noted, however, that national laws may limit the extent to which employees can be held liable for wrongful acts committed in the course of their duties. For example, article 18 of the Belgian Employment Contracts Act provides that employees shall remain exempt from *civil* liability except in case of "fraud, gross negligence or habitual light negligence".[281]

155. DISREGARD FOR INSTRUCTIONS – The question may arise whether an employee might be considered a controller if he or she decides to use personal data for his or her own purposes. According to the Article 29 Working Party,

> "*[s]pecial analysis is needed in cases where a natural person acting within a legal person uses data for his or her own purposes outside the scope and the possible control of the legal person's activities. In this case the natural person involved would be controller of the processing decided on, and would bear responsibility for this use of personal data. The original controller could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.*"[282]

156. ASSESSMENT – Article 16 of Directive 95/46 prohibits any person "acting under the authority of the controller" from processing personal data "except on instructions from the controller, unless he is required to do so by law". The employee who decides to use personal data for his or her own purposes may indeed be considered as a controller in his own right, by virtue of determining his own "purposes and means" of the processing. In my opinion, data subjects may in principle also seek compensation from the organisation under whose authority the personal data was being processed - even if the employee processes the data for purposes "outside the scope of the organisation's activities". This is a result of the strict liability regime of article 23 and the general rules of liability for actions undertaken by agents and auxiliaries.[283] In practice, this means that the data subject will generally have the choice whether or not to sue both parties

[279] Opinion 1/2010, *l.c.*, p. 15. See also M.B.J. Thijssen, *De Wbp en de vennootschap*, Kluwer, Deventer, 2009, p. 106-107.
[280] See e.g. articles 38-39 of the Belgian Data Protection Act.
[281] See also H. Cousy and D. Droshout, "Fault under Belgian Law", *l.c.*, p. 30.
[282] Opinion 1/2010, *l.c.*, p. 16.
[283] See also *supra*; nr. 134.

and whether or not to do so simultaneously or consecutively (although national tort law may specify otherwise).[284] Under Belgian law, the organisation shall be able to obtain redress from his employee where his actions constituted fraud, gross negligence or habitual light negligence.[285]

157. DIRECTOR LIABILITY – The directors of a company may also face civil or criminal liability for data protection violations. For example, section 61(1) of the UK Data Protection Act provides that

> "*Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.*"[286]

Under certain conditions, crimes committed by directors may also be attributable to the legal person, depending on national legislation.[287]

5.2 BRANCHES, DEPARTMENTS AND SUBSIDIARIES

158. OUTLINE – Large corporations and public bodies typically consist of multiple departments. In addition, large corporations may have multiple physical locations ("branches") in several different countries. A corporation may also be part of a larger concern, whereby its primary shareholder may be a parent or holding company. In practice, such configurations may make it difficult to determine which actor should be labelled as the "controller".[288] To what extent can the branch of a company, which does

---

[284] In Belgium, victims of concurrent faults may hold both the tortfeasor and the vicariously liable party liable *in solidum*. See H. Cousy and D. Droshout, "Multiple Tortfeasors under Belgian Law", *l.c.*, p. 33-35 and H. Cousy and D. Droshout, "Belgium", *l.c.*, p. 68-69.

[285] See also E. Dirix, "Aansprakelijkheid van en voor hulppersonen", *l.c.*, p. 346; L. Wynant, "Aansprakelijkheid voor en van derden die voor de vennootschap werken: Personeel ter beschikking stellen van werknemers, onderaannemers", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, 2000, p. II.3-41 and M. Lauvaux, "De burgerlijke aansprakelijkheid van werknemers", *Oriëntatie (Or.)* 2005, afl. 3, p. 69-71.

[286] The Belgian Data Protection Act does not explicitly target directors in its criminal provisions. They may, however, face criminal liability as "representatives" or "appointees" of the company. For more information see D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 362-379 (who observes that the Belgian legislator has been rather unclear with respect to which individuals might specifically be envisaged by the Act's criminal provisions).

[287] Opinion 1/2010, *l.c.*, p. 16-17. For the situation under Belgian law see H. Cousy and D. Droshout, "Liability for Damage Caused by Others under Belgian Law", *l.c.*, p. 41-42.

[288] See e.g. M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.,* p. 387 et seq.; M.B.J. Thijssen, "Data Protection and group companies", 17th BILETA Annual Conference April 5th - 6th, 2002, 12p.; C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 70-71; G.-J. Zwenne, A-W. Duthler, M. Groothuis a.o., "Eerste fase evaluatie Wet bescherming persoonsgegevens Literatuuronderzoek en knelpuntenanalyse", Ministerie van Justitie (NL), 2007, p. 100 and L. Moerel, "Back to basics: when does EU data protection law apply?", *International Data Privacy Law* 2011, Vol. 1, No. 2, p. 99-100.

not enjoy separate legal personality, be considered a controller"? Can a subsidiary, despite the existence of a hierarchical relationship with a parent company, be considered as a controller? Likewise, can an administrative department of a public body be its own controller, despite its formal dependence on a ministry or other administrative body?

A. An (over)emphasis on legal personality?

159. EMPHASIS ON LEGAL PERSONALITY – Despite the open-ended language of article 2(d), certain commentators argue that legal personality should be decisive when determining whether or not an entity can act as a "controller".[289] Under this approach, branches or organisational departments without separate legal personality in principle cannot be considered as controllers. The argument in favour of this approach is essentially two-fold. First, it is argued that only natural or legal persons can be holders of rights and obligations. Second, the actions of branches and organisational departments are ultimately attributed to the legal person under which they reside in accordance with rules of civil and corporate law. As noted by Moerel

> "*Only formal (legal) persons can have rights and obligations. In the case of a branch this would be the parent entity (to avoid one natural person within the branch being personally accountable for the processing of its employer). Any claim could only result in legal liability if it were brought against the legal entity controlling (under corporate law) the controller (under data protection law). Thus legal certainty would be best served if only the formal (legal) person being responsible for the processing at hand could qualify as a controller.*"[290]

160. PRAGMATIC APPROACHES – Other commentators have argued that it would not be appropriate to hinge the question of "who is the controller?" entirely on the question of legal personality. For example, Bainbridge has argued that

> "*It would be sensible if the acid test of who should be a controller was based on legal personality. However, this may not always be appropriate. A local authority has but one legal personality, as a corporation. This is unlike the group of companies where each has its distinct and separate legal personality. On the other hand, a partnership does not have its own legal personality distinct from its partners and it would be ridiculous if each partner had to register separate as a controller. In practice there may be some leeway and it may be up to organisations with complex structures to decide how to approach this issue.*"[291]

---

[289] L. Moerel, "Back to basics: when does EU data protection law apply?", *l.c.*, p. 99. In the same vein: Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 56.
[290] L. Moerel, "Back to basics: when does EU data protection law apply?", *l.c.*, p. 99.
[291] D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 118.

Bainbridge goes on to argue that large organisations which are a single legal entity but have several branches or departments may choose whether to operate the whole organisation as a single controller or to set up each branch office or department as a controller in its own right.[292]

161. PUBLIC VS. PRIVATE SECTOR – In her 1995 Ph.D. thesis, Overkleeft-Verbrug argues that the concept of a "controller" should be interpreted in accordance with the basic principles of private and public law.[293] Under private law, only natural or legal persons are recognized as legal subjects (i.e. can be holders of rights and obligations). As a result, she argues, only natural or legal persons can be "controllers" in the private law context.[294] Under public law, however, the main legal subject of regulation is not the legal person but rather the "competent body" (in Dutch: "*bevoegd orgaan*") as defined by administrative and public law.[295] This could be a Minister, but it might also for example be a City Council of Aldermen.[296] It stands to reason, therefore, that when the EU legislature adopted the terms "*public authority, agency or any other body*", it did so to accommodate the myriad of subjects recognized by Member States' public and administrative law, rather than to invent a new category of legal subjects.[297]

162. ASSESSMENT – The issue of whether or not an entity without legal personality may be considered a "controller" is not merely academic. It may have practical implications in terms of applicable law, transparency of processing and data subject rights. The wording of article 2(d) suggests that the EU legislator intended to bring entities without legal personality within the scope of this article. On the other hand, it is clear that branches and departments in principle act under the authority of the company or public body that created them. In addition, it seems reasonable to argue that EU legislature would have sought to align the concept of the controller with existing concepts of private and public law as much as possible. For the public sector, this means that the controller shall in principle be the "competent body", i.e. the entity which (according to public law and administrative law) is in charge of the natural person(s) or department(s) engaged in the processing of personal data.[298] In the private sector, the controller shall in principle be the entity (natural or legal person) under whose authority the processing of personal data is taking place, rather than the natural person(s) or branch(es) tasked with implementing the processing.[299]

---

[292] *Ibid*, p. 118-119.
[293] M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 378-381.
[294] *Ibid*, p. 387.
[295] *Ibid*, p. 379. See also U. Dammann and S. Simitis, *EG-Datenschutzrichtlinie*, *o.c.*, p. 112.
[296] *Ibid*, p. 387.
[297] In this regard, it is also worth noting that the initial proposal of the European Commission for Directive 95/46 had assimilated the wording of Convention 108, which defined the controller of the file as "*the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide* […]".
[298] *Ibid*, p. 387.
[299] *Ibid*, p. 387-388. See also Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free

B. Corporate concerns

163. PROBLEM STATEMENT – Multinational corporate concerns typically comprise a number of distinct legal persons, which may include one or more parent companies, holding companies and subsidiaries. In practice, the decision is sometimes made to endow one of these legal persons (e.g., the parent company or a subsidiary) with decision-making power regarding the processing of personal data on behalf of the corporate concern.[300] The legal person in question might even be formally designated as the "controller" of the corporate group. Such configurations give rise to several questions: to what extent are corporate actors able to freely designate the controller of the processing? Second, should a parent company not always be viewed as the controller in relation to processing undertaken by a subsidiary?

164. GENERAL CRITERIA APPLY – First off, it should be recalled that the general criteria of article 2(d) apply irrespective of whether the entities involved in the processing of personal data belong to the same corporate group. Any entity that determines the purposes and means of the processing of personal data shall be considered a controller, regardless of its corporate ties. In principle, the controller of a particular processing operation shall be the legal person under whose authority the processing is taking place.[301] Legal persons belonging to the same corporate group may, however, decide to pool certain resources or functions. In such cases, the legal persons involved will typically be considered as either "joint controllers" or "collaborating single controllers", depending on the circumstances.[302]

165. FORMAL DESIGNATION – Directive 95/46 does not explicitly prohibit arrangements (e.g., contracts or articles of incorporation) which designate one (or more) legal person(s) as "controller(s)" on behalf a corporate concern.[303] As is the case for controller-processor arrangements, however, the existence of a formal designation is not decisive. Such arrangements will only be recognized insofar as they are not contradicted by the facts.[304] Where there is reason to believe that the formal designation

---

movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 10 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 46 . See also *supra*; nr. 151.

[300] A "corporate concern" does not have separate legal personality and therefore cannot be considered as a controller within the meaning of article 2(d).

[301] M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.,* p. 387-388; Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 56 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 48-49.

[302] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 58 and D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 48-49.

[303] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 56.

[304] In the same vein: D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 49 with reference to J. Dumortier, "De toepassing van de Privacywet bij het personeelsbeheer: een stand van zaken", *Oriëntatie* (Or.) 1994, Nr. 11, p. 222.

does not correspond with the reality in terms of actual control, the arrangement may be set aside by the adjudicating body.[305] Only if the legal person in question actually determines the purposes and means of the processing, shall the arrangement enjoy full legal effect.

166. CORPORATE CONTROL – The concept of "control" under data protection law is a very different concept than "control" under corporate law.[306] The existence of a hierarchical relationship between corporate entities (control in the corporate sense) is not determinative for "control" in the data protection sense.[307] Parent companies are therefore not automatically considered "controllers" of the processing activities undertaken by their subsidiaries. At the same time, a parent company cannot exempt itself from its own data protection responsibilities simply by designating one of its subsidiaries as controller for the whole corporate concern. Again, the factual influence over the processing remains determinative.[308]

C. Governmental bodies

167. DESIGNATION BY NATIONAL OR COMMUNITY LAW – Article 2(d) provides that

> "*where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".

Processing of personal data by public bodies requires a legal basis. Ideally, when the legislature passes a law which requires the processing of personal data, it would indicate which entity shall act as a controller. In practice, however, this is seldom the case. As observed by the Article 29 Working Party:

> "*The explicit appointment of the controller by law is not frequent and usually does not pose big problems. In some countries, the national law has provided that public authorities are responsible for processing of personal data within the context of their duties. However, more frequent is the case where the law, rather than directly*

---

[305] Cf. supra; nr. 85. See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.,* p. 384.

[306] C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 71

[307] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 56-57 and M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.,* p. 388.

[308] See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.,* p. 384 and p. 397-398. An interesting question to consider in this regard is whether the "single economic entity doctrine", applied in competition law, could also be applied in data protection matters by way of analogy. Under the single economic entity doctrine, companies which form part of the same "economic unit" may be held responsible for the acts of other entities within the economic unit even if they have not participated in the infringement. (A. Jones and B. Sufrin, *EU Competition Law – Texts, Cases and Materials*, Oxford, Oxford University Press, Fourth Edition, 2011, p. 137. See however also O. Odudu and D. Bailey, "The single economic entity doctrine in EU competition law", *Common Market Law Review* 2014, Vol. 51, p. 1721-1758.)

appointing the controller or setting out the criteria for his appointment, establishes a task or imposes a duty on someone to collect and process certain data."[309]

168. "COMPETENT BODY" – In cases where the national or EU legislature has not explicitly designated the controller(s), but merely entrusted the processing of personal data to a particular governmental body, it may generally be assumed that the body in question is to be considered as "controller".[310] This viewpoint has been confirmed by the Article 29 Working Party as follows

> "*For example, this would be the case of an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, and sets up a register with a view to fulfil them. In that case, it follows from the law who is the controller. More generally, the law may impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as the controller for any processing of personal data in that context.*"[311]

In practice there may still be instances in which it is difficult to determine which governmental body (or bodies) is acting as the controller of the processing. For instance, several governmental entities might be charged with complementary tasks of public interest. This, in turn, might require multiple governmental entities, each within their respective domain, to carry out certain processing operations. If there is no clear specification in the law as to which entity shall act as a controller, their respective roles are determined by the general criteria of the Directive (purposes, means).[312]

5.3 THE ROLE OF "THIRD PARTIES" AND "RECIPIENTS"

169. OUTLINE – In addition to the three main actors (i.e. controller, processor and data subject), Directive 95/46 also recognizes two other actors, namely "third parties" and "recipients". Both concepts have received relatively limited attention in the literature.[313] The following sections will briefly elaborate upon the meaning of these

---

[309] Opinion 1/2010, *l.c.*, p. 10

[310] D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 51; D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, p. 35. See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 385-386 and Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 57.

[311] Opinion 1/2010, *l.c.*, p. 10

[312] [312] B. Van Alsenoy, E. Kindt and J. Dumortier, "Privacy and data protection aspects of e-government identity management", in S. Van der Hof, M.M. Groothuis (eds.), *Innovating Government - Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series (IT & Law), Vol. 20, T.M.C. Asser Press, Springer, 2011, p. 263-264. See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 57.

[313] A notable exception is the contribution by J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *International Data Privacy Law*, 2014, Vol. 4, No. 3, p. 177-188.

concepts, their role within the regulatory framework of Directive 95/46, as well as the importance of distinguishing between them.

A. Third party

170. DEFINITION OF A "THIRD PARTY" – Article 2(f) defines a third party as

> "*any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data*"

According to the Article 29 Working Party, the Directive uses the concept of a "third party" similarly to how this concept is normally used in civil law, where a "third party" refers to a subject which is not part of an entity or of an agreement.[314] In the data protection context, a "third party" should be understood as referring to any party which is not part of the "inner circle" of a particular data processing, which includes only the data subject, the controller and possibly a processor, as well as their respective employees.[315]

171. EXTERNAL TO DATA CONTROLLER AND PROCESSOR – Article 2(f) defines "third party" in a negative fashion: it refers to entities *other than* the data subject, controller, processor or their employees.[316] It is in fact a "residual" category.[317] Because a third party is not part of the "inner circle" of a particular data processing, it does not *a priori* enjoy any legitimacy or authorization for processing personal data.[318] Instead, a third party receiving personal data should in principle be viewed as a controller in his own right, which is separately responsible for ensuring compliance with the provisions of Directive 95/46.[319]

172. EMPHASIS ON LEGAL PERSONALITY – In private law context, legal personality shall in principle be determinative to determine whether or not an entity should be considered as a "third party" or not.[320] As a result, persons working for a separate organisation, even if they belong to the same group or holding companies would be considered "third parties". On the other hand, branches processing customer information under the direct authority of their headquarters would not be considered

---

[314] Opinion 1/2010, *l.c.*, p. 31.
[315] *Ibid*, p. 8.
[316] D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 55.
[317] Opinion 1/2010, *l.c.*, p. 35.
[318] *Id*.
[319] *Ibid*, p. 31.
[320] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 64. Regarding the distinction between public and private sector see also supra; nrs. 161 et seq.

third parties.[321] For the same reason, employees of either the controller or processor shall in principle not be considered as "third parties".[322]

173. ROLE OF THE CONCEPT – The Directive uses the concept of a "third party" in several provisions. It is mainly used with a view *to establish prohibitions, limitations or obligations* in cases where personal data might be processed by parties not envisaged at the moment of initial collection.[323] For example, recital (39) provides that

> "*Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party*".[324]

The third party concept plays a similar role in relation to the right to correction[325] and the right to object[326]. Article 7 (legitimacy) explicitly recognizes the interests of third parties to whom the data might be disclosed.[327] Article 8 (sensitive data), on the other hand, prohibits disclosure of sensitive data by certain bodies without the consent of the data subject. [328] Finally, the concept of a third party also plays a small role in relation to international data transfers.[329]

---

[321] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 11. See also Opinion 1/2010, *l.c.*, p. 31 and European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Data Protection Law*, 2014, p. 54, accessible at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf (last accessed 8 October 2015).

[322] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 64.

[323] Opinion 1/2010, *l.c.*, p. 31

[324] See also article 11(1) of Directive 95/46.

[325] Article 12(c) provides that Member States must guarantee that every data subject shall have the right to obtain from the controller "*notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort*".

[326] Article 14(b) provides that Member States shall grant the data subject the right "*to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.*"

[327] Article 7(e) provides that personal data may be processed if the "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed*" . Article 7(f) allows the processing of personal data if the "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).*"

[328] Article 8(2)d provides that the general prohibition regarding the processing of "*special categories of data" shall not apply where the "processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the*

B. Recipient

174. DEFINITION OF RECIPIENT – According to article 2(g), a "recipient" shall mean

> "*a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients*"

The term "recipient" should in principle be understood in its natural language meaning. It refers to *any* entity to whom data are disclosed. "Disclosure" should also be interpreted broadly in this context, referring to any type of divulgation of data regardless of the medium or modalities. For example, granting online remote access to data should in principle also be considered as form of disclosure.[330]

175. INTERNAL OR EXTERNAL TO CONTROLLER OR PROCESSOR - The concept of a "recipient" is much broader than the concept of a third party.[331] It may be an entity outside the organisation of the controller or processor (in which case the recipient is also a "third party"), but it may also be an entity who is part of the controller or processor, such as an employee or another division within the same company or department.[332]

176. ROLE OF THE CONCEPT – The term "recipient" was introduced primarily to help ensure *transparency* of processing towards data subjects.[333] For example, articles 10 and 11 stipulate that the data subject must in principle be informed of the "recipients or categories of recipients" of his data, insofar as such information is necessary to guarantee fairness of processing.[334] Data subjects who exercise their right of access must be provided with information at least as to "*the recipients or categories of recipients to whom the data are disclosed*".[335] Finally, controllers are likewise required to notify their

---

members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects."

[329] Article 26(1)(c) provides that that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may nevertheless take place on the condition that the "*transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party*."

[330] D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 56.

[331] European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Data Protection Law*, o.c., p. 54.

[332] *Id.* See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 64.

[333] Council of the European Union, Common position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/.../EC of the European Parliament and of the Council of ... on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* 13 April 1995, C 93, p. 22. Articles 10 and 11, for instance, may require controllers to inform data subjects of the "recipients or categories of recipients" of their personal data.

[334] See articles 10(c) and 11(1)c of Directive 95/46.

[335] See article 12(a) of Directive 95/46.

supervisory authority of the recipients or categories of recipients to whom the data are disclosed.[336]

177. EXCLUSION OF "AUTHORITIES" – Article 2(g) *in fine* provides that "authorities" which may receive data "in the framework of a particular inquiry" shall not be regarded as recipients. The Belgian Data Protection Act further clarifies that the "authorities" envisaged here are judicial or administrative authorities.[337] The reference to "a particular inquiry" further suggests that the exclusion only concerns disclosures which are of a limited and specific (as opposed to systemic) nature. Examples might include a targeted fiscal inspection or a judicial inquiry.[338] According to De Bot, the rationale for the exclusion is that such disclosures by definition cannot be anticipated at the moment of collection. As a result, it would not make sense to require controllers to mention such recipients (either towards data subjects at the moment of collection or towards supervisory authorities as part of a notification).[339] Bulk disclosures of personal data between public administrations, outside the context of a specific inquiry, shall in principle not be covered by the exclusion.[340]

C. Importance of the distinction

178. LEGITIMACY OF DISCLOSURE – The main difference between "third parties" and "recipients" concerns their relationship to the controller and their authorization to access personal data held by the controller.[341] A recipient may belong to the "inner circle" of a particular data processing, by being part of the organisation of either controller or processor. A disclosure to recipients therefore does not *ipso facto* require an additional legal basis.[342] A third party, on the other hand, is by definition external to the organisation of a controller. Disclosing personal data to a third party will therefore always require an additional legal basis.[343]

179. APPLICABLE REQUIREMENTS – "Third parties" to whom personal data are disclosed are by definition "recipients", but not all "recipients" are by definition third

---

[336] See articles 18(2) and 19(1)d of Directive 95/46.
[337] See article 1, §7 of the Belgian Data Protection Act.
[338] D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 57.
[339] *Ibid*, p. 57-58.
[340] See also the Judgement in *Smaranda Bara and Others*, C-201/14, EU:C:2015:638. Interestingly, the issue of whether the CNAS might be considered an "authority" within the meaning of article 2(g) was not even considered by either the Advocate General or the Court of Justice.
[341] European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Data Protection Law*, *o.c.*, p. 54.
[342] *Id.*
[343] *Id.* ("*The employees of a controller or processor may without further legal requirement be recipients of personal data if they are involved in the processing operations of the controller or processor. On the other hand, a third party, being legally separate from the controller or processor, is not authorised to use personal data processed by the controller, unless on specific legal grounds in a specific case. 'Third-party recipients' of data will, therefore, always need a legal basis for lawfully receiving personal data.*")

parties.[344] Every disclosure to a "third party" must therefore comply with provisions regarding third parties and recipients (but not *vice versa*). A processor is always deemed a recipient, but never a third party.[345]

D. A "third group" among those processing personal data?

180. A "THIRD GROUP"? – Salom argues that the concept of a "*third party to whom personal data are disclosed*", which is mentioned in article 7(f), should be considered as a separate category of actor which is distinct from controller and processor.[346] According to Salom, article 7(f) allows

> "*third parties to whom the data are disclosed [...] to process personal data to satisfy a legitimate, unique, and personal interest, however, they must adapt data processing to the purposes and means determined by another entity that controls that process.*"[347]

Salom categorically rejects the notion that a third party should be in principle be viewed as a controller in his own right:

> "*Interpreting that the role of the third party is an interim situation, at the end of which this party will become data controller or data processor depending on the circumstances, is not admissible because the contrast arising between the terms 'data controller' and 'third party' makes this impossible and, moreover, the definition itself of data controller given in Article 2 (d) also prevents undefined situations from arising temporarily.*"[348]

Examples of such "third parties to whom data are disclosed" are providers of telecommunications or electronic mail service, credit bureaus, list brokers and internet search engines.[349]

181. RATIONALE – At least part of Salom's rationale for carving out a "third group" stems from the difficulties that arise when trying to subject anyone who processes personal data to the legal regime applicable to controllers or processors.[350] Recognition of the "third group" would allow certain data disclosures to take place without bringing its recipients within the direct purview of Directive 95/46. Salom's main argument appears to be that the interests of data subjects are sufficiently protected by the obligations incumbent upon the controller in case of disclosure to a third party, i.e. prior

---

[344] D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 57.
[345] *Ibid*, p. 55.
[346] J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 177-188.
[347] *Ibid*, p. 179-180.
[348] *Ibid*, p. 179. Contra: Opinion 1/2010, *l.c.*, p. 31.
[349] *Ibid*, p. 183-187.
[350] *Ibid*, p. 177.

information, rights of rectification, cancellation and opposition.[351] In addition, recognition of the "third group" would resolve the legal questions and problems that arise when treating all "third parties to whom data are disclosed" as either controllers or processors.[352]

182. ASSESSMENT – While both intriguing and innovative, I do not find the argumentation advanced by Salom convincing. First, the provisions of Directive 95/46 are written mainly from the perspective of a particular processing operation, as undertaken by a particular controller at a particular moment in time. The textual arguments provided by Salom therefore do not preclude that a "third party to whom data are disclosed" might also, upon receipt, be considered a controller in his own right. Second, the provisions of the Directive which concern disclosures to third parties were not introduced with a view of limiting the obligations of certain entities. Rather, they were introduced because disclosures to third parties were viewed as presenting greater risks to data subjects, requiring additional (rather than less) safeguards.[353] Third, Salom does not offer clear criteria to distinguish between, on the one hand, a third party who merely has a "legitimate interest" and, on the other hand, a third party who determines his own purposes and means.[354] Fourth, the approach advanced by Salom would prevent data subjects from exercising their rights directly against the third party in question, even though data subjects might benefit from the ability to do so.

5.4 SUB-PROCESSING

183. A PLURALITY OF PROCESSORS – In Opinion 1/2010, the Article 29 Working Party noted that controllers increasingly outsource the processing of personal data to a plurality of processors.[355] The processors in question may each have direct relationship with the controller, or be sub-contractors to which a processor has delegated part of the processing activities entrusted to it ("sub-processors").[356] The possibility of sub-processing was also explicitly recognized in the context of the 2010 standard contractual clauses for international data transfers.[357]

---

[351] *Ibid*, p. 181-183.
[352] *Ibid*, p. 188.
[353] See e.g. Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, *l.c.*, p. 23.
[354] See J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 181.
[355] Opinion 1/2010, *l.c.*, p. 27.
[356] *Id*.
[357] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), 2010/87/EU, O.J. 12 February 2010, L 39/5-18. Since then, the Article 29 Working Party has developed draft ad hoc contractual clauses for subprocessing from EU based-processor to non-EU based sub-processors: see Article 29 Data Protection Working Party, "Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor", WP 214, 21 March 2014.

184. BOUND BY INSTRUCTIONS – Sub-processors are in essence subject to the same rules as processors. To retain their status as "processor", they must abide by the controller's instructions at all times.[358] The subprocessing contract between processor and subprocesor should also formally bind the subprocessor to adhere to the controller's instructions, as well as to implement the appropriate technical and organisational security measures.[359]

185. AGREEMENT OF THE CONTROLLER – A processor may only enlist a sub-processor with the prior written consent of the controller.[360] The ability to subcontract a whole or part of the processing may be specified in the initial processing agreement (between controller and processor), or may be agreed upon at a later stage. As to the level of detail, the Working Party considers that

> *"while it is not necessary that the controller defines and agrees on all the details of the means used to pursue the envisaged purposes - it would still be necessary that he is at least informed of the main elements of the processing structure (for example, subjects involved, security measures, guarantees for processing in third countries, etc), so that he is still in a position to be in control of the data processed on his behalf."*[361]

The Working Party also considers it necessary that there be a clear duty for the processor to name all subcontractors involved and to inform the controller of any intended changes. [362] In addition, the controller should at all times retain the possibility to object to such changes or to terminate the contract.[363] Finally, the Working Party also recommends that the controller should enjoy contractual recourse possibilities in case of breaches of contracts caused by the subprocessors.[364]

186. GENERAL CONSENT POSSIBLE – While sub-processing in principle may not take place without the agreement of the controller, the Working Party appears to accept that

---

[358] Opinion 1/2010, *l.c.*, p. 27.
[359] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 63. See also Clause 11 of the Standard Contractual Clauses (for processors) of 5 February 2010.
[360] See also Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", WP 196, 1 July 2012 p. 10 and Information Commissioner's Office (ICO), "Outsourcing - A guide for small and medium-sized businesses", 28 February 2012, v1.0, p. 6, accessible at https://ico.org.uk/media/1585/outsourcing_guide_for_smes.pdf. Failure to seek prior approval of the controller would arguably constitute a violation of article 16 (processing - by virtue of disclosure) beyond instructions of controller
[361] Opinion 1/2010, *l.c.*, p. 27-28.
[362] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 10.
[363] *Id.*
[364] *Id.* See also Clause 11 of the Standard Contractual Clauses for (Processors) of 5 February 2010. For more information regarding the contractual elements to be included see also M. Schmidl, "The Challenges of Subprocessing and Suggested Solutions under German and EU Privacy Law", *Bloomberg BNA World Data Protection Report* 2013, Vol. 13, No. 2, p. 1-5.

a controller may provide a "general prior consent" to allow sub-processing.[365] According to the Article 29 Working Party

> "*it is up to the controller to decide if general prior consent would be sufficient or if specific consent is required for each new sub processing. This decision will probably vary depend on the context of the processing, the type of data (sensitive or not), and the level of involvement of the controller for this type of choice. Some controllers may decide that a full prior check of the identity of each sub processor is necessary while others may consider that prior information […], the duty to communicate the clause […] and the guarantee to have the same level of protection […] are enough.*"[366]

187. LIABILTY OF INITIAL PROCESSOR – The initial processor remains liable towards the controller for failure to fulfil his own data processing obligations under the contract.[367]

[365] Article 29 Data Protection Working Party, "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC", WP176, 12 July 2010, p. 5. See also B. Wojtan, "The new EU Model Clauses: One step forward, two steps back?", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 77.

[366] *Id.*

[367] Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 63. See also recital (18) of the Standard Contractual Clauses for (Processors) of 5 February 2010.

Chapter 5 ADDITIONAL FUNCTIONS OF THE CONTROLLER AND PROCESSOR CONCEPTS

188. OUTLINE – The qualification of an actor as either a controller or processor has implications beyond the allocation of responsibility and risk. To begin with, the qualification is essential to determine which national law(s) applies (apply) to the processing.[368] In addition, determining the appropriate qualification of the actors involved may also be necessary to comply with a number of substantive provisions, in particular provisions regarding (a) transparency of processing; (b) data subject rights; (c) balance of interests and (d) legal binding between controllers and processors.[369] The aim of this section is to briefly elaborate upon the additional functions which the controller and processor concepts fulfil within the regulatory scheme of Directive 95/46.

1 DETERMINATION OF APPLICABLE LAW

189. ESTABLISHMENT OF CONTROLLER – Article 4 (1) sets forth the various instances in which a Member State must apply the national laws it has adopted when implementing the Directive. One of the main factors in each of these instances is the territory in which the controller is established.[370] For example, article 4(1)a provides that Member States must apply their national data protection laws if

> *"the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State [...]".*[371]

The determination of applicable law under article 4(1)a thus depends on the identification of which entity is acting as a "*controller*", together with the physical locations of its "*establishment(s)*".[372] Equally important, however, is the reference to the

---

[368] See Opinion 1/2010, *l.c.*, p. 5.

[369] See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 381.

[370] For more information see Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", WP 179, 16 December 2010, p. 8, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf (last accessed 19 July 2013). In addition to these "main criteria", the Directive also specifies in article 4(1)(b) that Member States shall apply their national data protection laws when "*the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law*".

[371] Article 4(1)a of Directive 95/46 (emphasis added). This provision goes on to state that "*when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*".

[372] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 8. The notions of "controller" and "establishment" do not coincide. A controller can have several establishments, just as entities that jointly exercise control can concentrate activities within one or more establishments. (*Ibid*, p. 11.) The term "establishment" is not formally defined by Directive 95/46, but according to recital (19) "*implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment*". See also Judgement in *Google Spain*, C-131/12, EU:C:2014:317, at paragraphs 42 et seq; Judgment in *Weltimmo*, C-230/14, EU:C:2015:639, at paragraphs 24 et seq. and Article 29 Data

"*context of activities*": this criterion implies that the establishment of the controller must be involved in activities implying the processing of personal data in question.[373] Or rather, the establishment must be involved in a "*real and effective exercise of activities in the context of which the personal data are being processed*".[374]

190. USE OF EQUIPMENT – Article 4(1)c provides that Member States must apply their national data protection laws if

> "*the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State […]*"

Again, the determination of applicable law is dependent on the identification of which entity is acting as a "controller". Article 4(1)c only applies, however when the controller does *not* have any establishment on EU/EEA territory which may be considered "relevant" for the purposes of article 4(1)a.[375] According to the Article 29 Working Party, the term "equipment" should be given a broad interpretation, which comprises both human and technical resources.[376] More specifically, the Working Party understands the term "equipment" to have the same meaning as the term "means" used in article 2(d) of the Directive.[377] The concept of "making use", on the other hand, is given a slightly more narrow interpretation. According to the Working Party, this concept presupposes two elements: (1) some kind of activity of the controller and (2) a clear intention of the controller to process personal data.[378] While it is not required that the controller have

---

Protection Working Party, "Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, WP 179 update", 16 December 2015, p. 3 et seq. available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf (last accessed 28 April 2016).

[373] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 2.

[374] *Ibid*, p.11. According to the majority of doctrine and regulators, article 4(1)a does not require that the "establishment" in question is actually acting as a controller, nor that the processing itself takes place on the territory of the Member State in question (L. Moerel, "Back to basics: when does EU data protection law apply?", *l.c.,* p. 97. For an overview of divergent views see L. Moerel, "Back to basics: when does EU data protection law apply?", *l.c.*, p. 103 and Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 8.

[375] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 19. The application of article 4(1)c is not prevented if the controller only has an "irrelevant" establishment on EU territory. (*Id.*) The Article 29 Working Party has thus chosen to give this phrase a functional rather than literal interpretation of the phrase "*the controller is not established on EU territory*".

[376] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 20. The legislative history of Directive 95/46 suggests that its drafters only had physical objects in mind when using the word "equipment". (See L. Moerel, "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *l.c.*, p. 33 and 36). However, in its 2008 opinion on applicable law the Working Party clearly embraced a broader notion of the term "equipment" by equating this term to the concept of "means".

[377] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 20.

[378] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", *l.c.*, p. 20; Article 29 Data Protection Working Party, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", *l.c.*, p. 9.

ownership or full control over the equipment in question, it is necessary that the controller have a sufficient "degree of disposal".[379]

191. ESTABLISHMENT OF PROCESSOR – The qualification of an actor as a processor can also be determinative in deciding which law to apply to a particular processing operation. Article 17(3) provides that the scope of the processor's security obligations shall be determined by the national law of the Member State where the processor is established. The rationale behind this provision is to ensure uniform requirements within one Member State with regard to security measures. Due to the fact that security requirements can diverge considerably among Member States, this may have practical implications.[380]

2 COMPLIANCE WITH SUBSTANTIVE PROVISIONS

2.1 TRANSPARENCY OF PROCESSING

192. IDENTITY DISCLOSURE – Articles 10 and 11 of the Directive, which set forth the information to be given by the controller to the data subject, specify that the data subject must in principle be informed of the identity of the controller and/or his representative.[381] When the processing involves multiple actors, compliance with this obligation will require them to formally establish the role of each actor in order to determine whether or not the data subject must be informed of their identity as such.[382] As a rule, the identity of any controller(s) involved in the processing must always be disclosed. In contrast, the identity of the processor must not necessarily be communicated to the data subject, unless such disclosure may be deemed necessary in order to guarantee fair processing in respect of the data subject.

---

[379] Article 29 Data Protection Working Party, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", *l.c.*, p. 9. See also L. Moerel, "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *l.c.*, p. 37. A sufficient degree of disposal is said to be present "*if the controller, by determining the way how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing. In other words, the controller determines, which data are collected, stored, transferred, altered etc., in which way and for which purpose*." (Article 29 Data Protection Working Party, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", *l.c.*, p. 9.)

[380] See Opinion 8/2010, *l.c.*, 25.

[381] Cf. *supra*; nr. 53 et seq.

[382] This shall particularly be the case where the notice that is provided to the data subject seeks to address the notice obligations of multiple controllers. This may be done for a variety of purposes, e.g. to address the fact that not every controller has the ability to communicate directly with the data subject at the moment of data collection.

2.2 *DATA SUBJECT RIGHTS*

193. ACCOMMODATION – The controller of the processing is obliged to accommodate data subject rights.[383] Even if he appoints a third party to act as a point of contact, he cannot escape the fact that he remains ultimately responsible for ensuring an appropriate accommodation data subject rights. The data subject may always approach the controller directly to request access, erasure or blocking. Determining the appropriate qualification of the actors involved is therefore necessary to properly organize the accommodation of data subject rights.

194. AUTHORITY TO DECIDE – The controller is in principle also the entity who has the authority to decide, in first line, whether to grant or refuse a request made by a data subject.[384] Pursuant to article 16, the processor may only process the data on instructions from the controller, unless he is required to do so by law. As a result, a processor may not accommodate data subject rights on his own initiative, without prior authorisation by the controller.

2.3 *BALANCE OF INTERESTS*

195. INTERESTED PARTIES – Article 7(f) puts forward a number criteria for making data processing legitimate.[385] Article 7(f) of Directive 95/46 makes reference to the legitimate interests pursued "*by the controller or by the third party or parties to whom the data are disclosed*". The potential interests of the processor are not mentioned. As a result, only the legitimate interests of the controller or of third parties to whom the data are disclosed may be taken into account when determining the legitimacy of processing pursuant to article 7(f).[386] Articles 7(e), 8(2)b and 8(5) similarly only make reference to the rights, obligations or authority of the controller, not of the processor.

2.4 *LEGAL BINDING*

196. CONTRACT OR OTHER ACT – Article 17(3) of the Directive stipulates that when a controller engages a processor to carry out certain processing operations on his behalf, their relationship must be governed by a contract or other legal act which contains certain mandatory provisions.[387] The qualification of an actor as either controller or processor therefore has immediate implications for the contractual arrangements that should be in place between the entities involved in the processing. The same also applies in the context of an international data transfer, where an appropriate qualification of

[383] See article 12 and 14 of Directive 95/46. See also *supra*; nr. 55 et seq.
[384] See also M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 381.
[385] Cf. *supra*; nr. 49.
[386] The same in principle applies when deciding whether to grant or refuse a request made by the data subject.
[387] Cf. *supra*; nr. 85.

each actor is necessary for determining what type of EU model contract should be used.[388]

[388] See also P. Van Eecke, M. Truyens et al. (eds.), "The future of online privacy and data protection", *l.c.*, p. 32 at note 162.

Chapter 6 CONCLUSION

197. ALLOCATION OF RESPONSIBILITY AND RISK – Within the regulatory scheme of Directive 95/46, the controller carries the primary responsibility for ensuring compliance. At the moment of its enactment, the EU legislature was mindful of the practice whereby one organisation requests another organisation to perform certain processing operations on its behalf. By introducing the concept of a "processor", the EU legislator hoped to be able address this situation and to ensure a continuous level of protection.[389]

198. RELATIONSHIP CONTROLLER-PROCESSOR – The Article 29 Working Party has approximated the relationship between controllers and processors with the figure of delegation. The analogy appears to be founded on a number of considerations. In first instance, a processor acts "on behalf" of a controller and is called upon to "implement the instructions given by the controller" (article 16).[390] Secondly, the consequences of the processor's actions are in principle attributed to the controller, provided that the processor merely follows the latter's instructions. Finally, the delegation figure also permits the delegate (processor) to exercise a certain amount of discretion on how to best serve the principal's (controller's) interests.[391]

199. MULITPLICITY OF CONTROL – Not every collaboration involving the processing of personal data among two separate actors implies the existence of a controller-processor relationship. It is equally possible that each actor processes personal data for their own distinct purposes, in which case each actor is likely to be considered a controller independently of the other. It is also possible that collaborating actors jointly exercise decision-making power concerning the purposes and means of the processing, in which case they are considered to act as joint or (co) controllers.

200. VARYING DEGREES OF CONTRACTUAL FLEXIBILITY – Directive 95/46 has devoted several provisions to the relationship between controllers and processors. Article 17(3) obliges controllers to conclude a contract with their processors, which must specify that the processor is obliged (1) to follow the controller's instructions at all times and (2) to implement appropriate technical and organisational measures to ensure the security of processing. In contrast, Directive 95/46/EC in principle does not contain any specific requirements aimed at regulating the relationship among

[389] The provisions which regulate the relationship between controllers and processors were in fact intended to ensure that such outsourcing arrangements did not result in a lowering of protection enjoyed by data subjects. Cf. *infra*; nr. 489.
[390] Opinion 1/2010, *l.c.*, p. 25.
[391] See Opinion 1/2010, *l.c.*, p. 25.

controllers as such.[392] The Article 29 Working Party has stated that they are free to determine how to best allocate responsibility amongst each other, "as long as they ensure full compliance".[393] The result is that collaborating (co-)controllers are in principle free to assign responsibilities, whereas controller-processor relationships must be modelled according to a pre-defined format.

201. VARYING LIABILITY EXPOSURE - Whether an actor is considered a controller, co-controller or processor has important implications in terms of liability exposure. Controllers can face liability not only for their own activities, but also for the activities of their processors. Processors, on the other hand, shall in principle only be indirectly accountable: Directive 95/46 does not afford data subjects with direct recourse against processors (although such recourse may be provided by national law). Liability exposure of different controllers working together may vary depending on whether or not they are seen to act as "separate" controllers or "joint" controllers. While Directive 95/46 explicitly recognizes the possibility of joint control, it did not specify how this relationship might affect each controller's liability exposure.

202. ADDITIONAL FUNCTIONS – The legal status of an actor as either a controller or processor is not only important for issues of liability, but also has important implications. First, the qualification of an actor as either a controller or processor is an essential element in determining which law(s) applies (apply) to the processing. Second, several other provisions of the Directive make explicit reference to either the "controller" or a "processor". This is quite natural, as these concepts serve primarily as vehicles to convey the respective obligations of these actors. However, for certain provisions of the Directive it is also necessary to know which role a particular actor has assumed towards the processing in order to be able to comply with them.[394]

[392] One notable exception has resulted from the administrative practice surrounding international transfers. Cf. *supra*; footnote 189.
[393] Opinion 1/2010, *l.c.*, 24.
[394] For instance, articles 10 and 11 of the Directive, which set forth the information to be given by the controller to the data subject, specify that the data subject must in principle be informed of the identity of the controller and/or his representative. When the processing involves multiple parties, compliance with this obligation will require them to formally establish the role of each actor in order to determine whether or not the data subject must be informed of their identity as such.

PART III

HISTORICAL-COMPARATIVE ANALYSIS

Chapter 1 INTRODUCTION

"*You have to know the past to understand the present*".

Dr. Carl Sagan, 1980[395]

203. PREFACE – The concepts of controller and processor were not created out of thin air. Prior to Directive 95/46, many other data protection instruments incorporated concepts with similar meaning and scope. The research objective of this Part of the thesis is to enhance the understanding of the meaning and role of the controller and concepts by tracing the origin and development of these concepts over time.

204. RELEVANT PERIODS – When one looks at EU data protection law from a historical perspective, four main periods can be distinguished, namely:

(1) the emergence of national data protection laws (1970-1980);

(2) internationalisation (1980-1981);

(3) national implementation (1982-1994);

(4) European harmonisation (1995-2016).

205. SELECTION CRITERIA – In principle, every data protection instrument adopted during each of the aforementioned periods is worthy of analysis. A selection must be made, however, if only for practical reasons. Two criteria have guided the selection made here, namely (1) the desire to be comprehensive (i.e. to avoid large gaps in terms of chronology); and (2) ease of access and language considerations.[396]

206. APPLICATION – For the first period, three data protection laws were chosen, namely the data protection laws of Hesse, Sweden and France. The Hessian and Swedish acts were chosen simply because they represent the very first national data protection laws. The French data protection act was selected to bridge the gap between the first data protection laws the first international instruments of data protection and on the basis of language considerations. For the second period, Convention 108 and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines") and Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ("Convention 108") were selected. An analysis of Convention 108 was deemed indispensable, as it provided the normative framework of the national implementations in the period that followed. The analysis of

[395] Carl Sagan, "One Voice in the Cosmic Fugue", *Cosmos*: Episode 2, available at https://www.youtube.com/watch?v=7-I7jP5fNcE (55:35) (last accessed 16 April 2016).

[396] For a discussion of potential selection criteria for comparative law purposes see A.E. Oderkerk, *De preliminaire fase van het rechtsvergelijkend onderzoek*, Ph. D. Thesis, 1999, Amsterdam Center for International Law (ACIL), p. 47-60 and p. 221-239.

the OECD guidelines was deemed beneficial as the Guidelines were developed in parallel with Convention 108, and therefore offer additional insights into the meaning of the concepts employed by Convention 108. For the third period, two data protection laws were selected, namely the 1984 UK Data Protection Act and the 1992 Belgian data protection. Again, this selection was driven by the desire to be comprehensive from a chronological perspective as well as by language considerations. Finally, Directive 95/46 and the GDPR were selected as the two instruments of European harmonisation simply because they are the focal point of this thesis.

207. SOURCES – The historical-comparative analysis conducted in this Part of the thesis shall be primarily dogmatic in nature. To the extent possible, the analysis shall be based on primary sources (i.e. legislation, formal declarations and guidelines issued by the relevant institutions). Where appropriate, however, reference may also be made to preparatory works and explanatory memoranda, jurisprudence, and doctrinal accounts.

208. ANALYSIS – Each of the selected instruments of data protection regulation will be analysed in a structured and focused manner.[397] Specifically, each instrument will include an analysis of:

(1) the origin and development of the instrument in question;

(2) its scope *ratione materiae*;

(3) its basic protections; and

(4) the manner in which and responsibility and risk is allocated (scope *ratione personae*).

With respect to the fourth element, the following questions will guide the analysis:

(1) how are actors and roles defined?

(2) how is responsibility and risk allocated among the identified actors?

(3) what is the threshold for responsibility and risk?

(4) how prescriptive is the regulation of the relationship among actors involved in the processing?

209. OUTLINE – Before delving into the analysis of specific national data protection laws, a brief overview shall be given of how European data protection laws came into existence. Next, three of the earliest data protection laws (i.e. of Hesse, Sweden and France) are analysed. After that, two international instruments of data protection are discussed, namely the OECD Guidelines on the Protection of Privacy and Transborder

[397] The analysis is "structured" in the sense that the analysis of each law is composed of the same subsection and seeks to answer the same questions in relation to each use case. The analysis is "focused" in that the analysis extends only to those aspects which are relevant for purposes of the research question which this Part seeks to address. Based on A.L. George and A. Bennet, *Case Studies and Theory Development in the Social Sciences*, *o.c.*, p. 67 et seq.

Flows of Personal Data ("OECD Guidelines") and Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ("Convention 108"). Next, two national data protection laws implementing Convention 108 are analysed, namely the UK and Belgian data protection acts, followed by a discussion of the legislative development of Directive 95/46. Finally, the General Data Protection Regulation (GDPR) and its legislative development will be analysed. By way of conclusion, a summary overview will be provided of how the controller and processor concepts evolved over time.

Chapter 2 THE EMERGENCE OF DATA PROTECTION LAW

1 HISTORICAL CONTEXT

210. INTRODUCTION – Data protection emerged as a policy issue in a time of profound social and economic change.[398] In the 1960s, as society continued its transition from an industrial to a post-industrial economy, many European nations introduced comprehensive social reforms.[399] Administering these reforms would oblige governments to collect and process significant amounts of data about their citizens.[400] Thanks to the advances in computing technology, governments would be able to process these data in an automated fashion. Initially, the use of computer applications had been confined to tasks related to research and planning.[401] Towards the middle of the 1960s, however, computers started to make their appearance in daily administration, thereby increasing public awareness.[402] This awareness in turn led to the realization that the application of information technology might alter the nature of the relationship between the individual and the state.[403]

211. CATALYSTS – The public debate regarding the use of automated data processing techniques was fuelled by a number of catalysts. First, several governments were developing plans for centralized and computerized *population data banks*.[404] These plans triggered public concerns regarding the ability of the state to infringe upon the privacy of its citizens, for example by creating "crib-to-grave dossiers", or by developing "comprehensive systems of data surveillance".[405] Closely related to this issue were the proposals to introduce (or extend the use of) *personal identification numbers* for citizens.[406] As these numbers facilitate the linkage of information across record-keeping systems, these proposals augmented the concern that governments might at some point start to use citizens' information against them. A third cause for public alarm were the

---

[398] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 14.
[399] V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, p. 222.
[400] *Id*.
[401] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 3-4.
[402] *Id*.
[403] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. ix.
[404] *Ibid*, p. 46-49. See also V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 222-223.
[405] R. Turn and W.H. Ware, "Privacy and Security Issues in Information Systems", *IEEE Transactions on Computers* 1976, Vol. C-25, No. 12, p. 153.
[406] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 49. See also G. Stadler and T. Herzog, "Data Protection: International Trends and the Austrian Example", Guest Seminar at the International Institute for Applied Systems analysis, Laxenburg, Austria, 1981, p. 5 and L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 94.

scheduled *population censuses*.[407] Several censuses scheduled around 1970 helped bring privacy questions to the public attention, both because of the seemingly intrusive nature of the questions asked, as well as the use of automation in the census processes.[408] Finally, an array of "*alarmist" publications* which emerged in the late 1960s and 1970s also served to draw public attention to the dangers computers might pose to the rights and freedoms of individuals.[409]

212. LITTLE BROTHER – Of course, the use of information technology was not limited to the public sector alone. Private sector entities were likewise exploring the use of automated data processing to improve the efficiency of their daily operations.[410] Many felt that individuals should also be protected from intrusive data processing carried out by private sector entities. However, the establishment of data protection rules for the public sector was generally regarded as the most urgent matter.[411] As a result, the earliest instruments of data protection regulation focused on the use of automated data processing by the public sector. Quite soon, however, legislative initiatives which encompassed private sector processing activities were being considered as well.[412]

2 RATIONALE

213. WHY DATA PROTECTION? – The growing use of computing applications was perceived as posing a threat to individuals' rights and freedoms, in particular their right to privacy.[413] This perception of risk was closely related to the new capabilities offered by emerging computing technologies.[414] First, computers were making it increasingly easy to aggregate large amounts of information.[415] Until then, records containing personal information generally remained scattered across different filing systems in different departments and organisations.[416] Simply finding a particular piece of

[407] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 51.
[408] *Id.*
[409] *Ibid*, p. 53.
[410] See e.g. A.R. Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society", *Michigan Law Review* 1969, vol. 67, p. 1105; F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 7-8; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 97-98.
[411] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 22-23.
[412] See F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 20 (Table 6).
[413] *Ibid*, p. 7 (noting that "The demand for appropriate measures was motivated not so much by indications that abuse had actually occurred but rather by the fear and risk of abuses".) See also the discussion of future risks in Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, 1975, La Documentation Française, Paris, p. 14-17.
[414] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 93. See also e.g. Home Office (Great Brittain), *Computers and Privacy*, Cmnd. 653, Her Majesty's Stationary Office (HMSO), London, 1975; reproduced by Home Office (Great Brittain), *Report of the Committee on Data Protection*, Cmnd. 7341, HMSO, London, 1978, p. 451.
[415] G. Stadler and T. Herzog, "Data Protection: International Trends and the Austrian Example", *l.c.*, p. 4-5.
[416] J. A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives*, Norwegian University Press, Oslo, 1986, p. 65.

information could be a challenge.[417] With the help of computers, however, the information retrieval process would be greatly facilitated and accelerated. Computers also made it easier and cheaper to store information. As a result, one could expect that, over time, more and more data would be recorded and that these records would be kept for increasingly long periods of time.[418] This information could in turn be made readily available to an increasing number of parties, who could use it for a variety of purposes.[419] The combination of these elements gave rise to a vision of a future in which the individual would become completely transparent; whereby personal freedom would be dependent on the outcome of obscure data processing practices.[420]

3 GOALS OF DATA PROTECTION REGULATION

214. OVERVIEW – The primary goal of data protection legislation is to protect individuals (and by extension, society) against harms resulting from the misuse of their personal data.[421] To this end, these laws have instituted a variety of procedural safeguards to protect individuals, in particular their right to privacy, in relation to such processing.[422] Generally speaking, one can discern three sets of interrelated goals underlying the provisions of data protection legislation, namely a desire to[423]:

1. Protect individuals' privacy and related societal values;
2. Enhance the accountability of record-keepers and users of personal information; and
3. Improve the integrity and efficiency of decision-making processes.

---

[417] *Id.*

[418] See C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 17 (citing P. Sieghart, *Privacy and Computers*, London, Latimer, 1976, p. 75-76).

[419] *Id.*

[420] See also L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 94-95. In 1968, one member of the UK Parliament "*could picture the stage being reached when a button was pressed and if the computer gave the "thumbs down" sign, he would never get a license*". (C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 45; citing M. Warner and M. Stone, *The Data Bank Society: Organisations, Computers and Social Freedom*, London, Allen & Unwin, 1970, p. 105)

[421] P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", *l.c.*, p. 76.

[422] *Ibid*, p. 77; P. De Hert and S. Gutwirth, "Data Protection and the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action", in S. Gutwirth, Y. Poullet, P. De Hert, J. Nouwt and C. De Terwangne (eds.), *Reinventing data protection?*, Springer Science, Dordrecht, 2009, p. 9.

[423] Based on C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 44; P. De Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", *l.c.*, p. 77; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 107-112. See also J. Bing, "A Comparative Outline of Privacy Legislation", *Comparative Law Yearbook* 1978, Vol. 2, p. 170 et seq., who differentiates between "the interest in adequate information", "the interest in discretion" and "the interest in being informed".

215. PRIVACY AND RELATED VALUES – Most data protection instruments identify privacy protection as one of the primary justifications for their enactment.[424] A shaky foundation, one might say, as the right to privacy is generally considered "notoriously difficult to define".[425] Over time, privacy has been construed in a variety of ways, most notably as (a) a right "to be let alone"; (b) limited access to the "self"; (c) confidentiality; (d) control over one's personal information; and (e) the ability to make personal choices and develop relationships without undue interference.[426] Privacy is also generally considered instrumental for the protection of a range of related societal values, such as individuality, autonomy and dignity.[427] While there is no consensus regarding a definition of the right to privacy, the various conceptualizations have – to a lesser or greater extent – found their application in provisions of data protection regulation.[428] For example, the data subject rights of erasure or blocking[429] can be seen as (partial) manifestations of a right to control the circulation of one's personal information. Similarly, the special treatment of certain types of "sensitive" data (e.g., data relating to health or sex life)[430], can be seen as an effort to limit access to individuals' more intimate personal details.[431] None of the aforementioned conceptualizations of privacy can, however, provide a comprehensive (let alone exhaustive) account of all the rights and obligations found in data protection law.

216. KNOWLEDGE IS POWER – A second set of concerns surrounding the increase in computer usage revolved around the issue of information asymmetry. While individuals were becoming increasingly transparent, the organisational practices involving their personal data were becoming increasingly opaque. This was perceived as a threat to the balance of power that existed between individuals, organisations and governments.[432]

---

[424] See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 170.

[425] See e.g. P.E. Agre, "Introduction", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, p. 6; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 126.

[426] For a comprehensive overview of the various meanings attributed to the concept of privacy see D. Solove, "Conceptualising Privacy", *California Law Review* 2002, Vol. 90, p. 1087-1155. See also L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 125 et seq; P.E. Agre, "Introduction", *l.c.*, p. 6-7.

[427] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 133-136. Privacy is at times also seen as a necessary condition for the effective enjoyment of other fundamental rights, such as the freedom of expression.

[428] See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 174-175.

[429] See e.g. article 12(c) of Directive 95/46/EC.

[430] See e.g. article 8 of Directive 95/46/EC.

[431] For a more comprehensive account of the legal manifestations of the various conceptualizations of privacy and related societal values see L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 153-156.

[432] G. Stadler and T. Herzog, *l.c.*, p. 4; R. Turn and W.H. Ware, *l.c.*, p. 1354; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 107. For a more detailed treatise of "information as power" see also P. Seipel, "The Right to Know - Computers and Information Power", in P. Blume (ed.), *Nordic Studies in Information Technology and Law*, Computer/Law series n° 7, Kluwer, Deventer, 1991, p. 7-43. Some were also fearful that computers might unduly strengthen the power of the executive vis-à-vis the legislative branch of government, as evidenced by the Hessian Data Protection Act. See F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 5-6 and H. Burkert, "Privacy - Data Protection A German/European Perspective", in C. Engel K.H. Keller (eds.), *Governance of Global Networks in the Light of*

The use of computing technology would make it much easier to collect and analyse personal data, thereby increasing record-keepers' abilities to surreptitiously manipulate individuals' behaviour or to exercise other forms of social control.[433] Many data protection laws have sought to mitigate these risks by introducing specific duties to inform and dedicated oversight mechanisms.[434] These measures can be seen both as efforts to reduce the information asymmetries among the various stakeholders (by imposing transparency) and/or as "checks" against abusive record-keeping practices (by enhancing the accountability of public and private record-keepers).[435]

217. DATA QUALITY – A third objective common to most data protection laws is improving the integrity and efficiency of decision-making processes.[436] The use of inaccurate, incomplete or irrelevant information in a decision-making process can be more detrimental to the individual concerned than a breach of confidentiality.[437] As computers made it easier to store information for prolonged periods of time, and to make the same information available to wide variety of users, the risk of harms resulting from the reliance upon erroneous data was expected to increase.[438] Several data protection requirements can be seen as efforts to "sanitize the informational environment"[439]; in particular those provisions which seek to impose limits upon the collection[440] and storage[441] of information, or provisions which require that recorded information be kept up-to-date[442] or limit the use of such data to a particular context.[443]

Differing Local Values, 2000, Nomos, Baden-Baden, p. 45, available at http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf (last accessed 12 March 2013).

[433] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 103 and 107; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 19 and 29; J. A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives*, *o.c.*, p. 60 and 64.

[434] See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 176-178 (relating such provisions to a general "interest in being informed").

[435] See also S. Rodotà, "Data Protection – Some problems for Newcomers", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 188. Of course, transparency and accountability are closely related to one and other: "what is in the dark cannot be scrutinized" (M. Hildebrandt and B.J. Koops, "The Challenges of Ambient Law and Legal Protection in the Profiling Era", *The Modern Law Review* 2010, p. 449. On the role of accountability as a data protection principle over time see also J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, Houndmills (UK), 2012, p. 49-82.

[436] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 44; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 105 et seq.

[437] See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 170-171 ("*One prime form of misuse is the use of non-relevant information in a decision process; or the negligence to take into consideration information which the person in question himself holds as relevant.*").

[438] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 35. See e.g. A.R. Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society", *l.c.*, p. 1114.

[439] L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 137.

[440] See e.g. article 6(1)c of Directive 95/46/EC.

[441] See e.g. article 6(1)e of Directive 95/46/EC.

[442] See e.g. article 6(1)d of Directive 95/46/EC.

4 NATIONAL AND INTERNATIONAL DEVELOPMENT

218. NATIONAL DATA PROTECTION LAWS BEFORE 1980 – The first data protection law was adopted at regional rather than national level, namely by the German Land of Hesse. The Hessian Act of 7 October 1970 was the first legislative act to establish data protection rules of general application.[444] The first national data protection law was adopted by Sweden in 1973, followed in 1978 by Germany, France, Denmark, Norway and Austria. By the end of 1970's a total of seven European countries had enacted general data protection laws.[445] In the following chapter, the data protection laws of Hesse, Sweden and France will be investigated as exemplifications of the regulatory approach embodied by the earliest data protection laws.

219. INTERNATIONAL INSTRUMENTS – Although individual accounts vary, the first discussions among international policymakers on the need for data protection may be situated towards the end of the 1960's.[446] By the beginning of the 1970's, both the Council of Europe and the OECD were engaged in dedicated efforts to evaluate the privacy issues related to data banks.[447] Eventually, those efforts resulted in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD) and the Convention for the protection of individuals with regard to automatic processing of personal data (Council of Europe), which were finalized in 1980 and 1981 respectively.

220. NATIONAL DATA PROTECTION LAWS AFTER 1981 – Following the adoption of Convention 108, several Member States of the Council of Europe enacted their first national data protection laws.[448] Despite the growing convergence among national data protection laws, notable differences remained, reflecting the different national traditions in policymaking, constitutional norms and socio-economic environments.[449]

---

[443] See e.g. article 6, 1(a) of Directive 95/46/EC. Of course, limitations upon the collection, storage and use of information can also be seen as an attempt to help secure privacy and related societal values (by imposing limits on the collection of privacy-sensitive information and reducing the risk that information be used out of context). However, it is clear that the drafter's of data protection laws were concerned with information quality in addition to privacy and integrity (see L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 137).

[444] M. D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy, *Stanford Journal of International Law* 1980, vol. 16, p. 39.

[445] N. Platten, "Chapter 2: Background to and History of the Directive", in D. Bainbridge, *EC Data Protection Directive*, Butterworths, London, 1996, p. 14.

[446] Compare e.g. F.H. Cate, "The EU Data Protection Directive, Information Privacy, and the Public Interest", *l.c.*, 431 with D. Campbell and J. Fisher (eds.), *Data transmission and privacy*, Center for International Legal Studies, Martinus Nijhoff Publishers, Dordrecht, 1994, vii.

[447] H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 51.

[448] For a chronological overview see C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, p. 57.

[449] For a detailed discussion of the different factors contributing to divergence see C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, p. 194 et seq. who describes five possible explanations for policy divergence: (1) formal constitutional norms; (2) preferences and influence of dominant social groups; (3) electoral politics and partisan ideology; (4) the position and power of national bureaucracies; and (5) economic constraints.

221. EUROPEAN HARMONISATION - By the mid-1980's it was becoming clear that further harmonization would be necessary in order to secure the proper functioning of the EU internal market.[450] In 1990, the European Commission put forth its first draft for a "Council Directive on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data", which eventually led to the adoption of Directive 95/46/EC.

[450] N. Platten, "Chapter 2: Background to and History of the Directive", *l.c.*, 23-24.

Chapter 3 NATIONAL DATA PROTECTION LAWS BEFORE 1980

222. OUTLINE – This chapter will analyse three of the earliest data protection laws, namely the Hessian Data Protection Act of 7 October 1970[451], the Swedish Data Act of 11 May 1973[452] and the French Law on Informatics, Files and Liberties of 6 January 1978[453]. The objective of this analysis is to ascertain how the early data protection laws allocated responsibility for complying with the norms they contained. For each instrument, the analysis will commence with a discussion of the origin and development of the instrument in question. Next, the scope *ratione materiae* of each instrument shall be discussed, followed by an overview of the basic protections it contains. Finally, a separate section shall be dedicated to an analysis of how each instrument allocates responsibility and risk for (non-)compliance.

1 THE HESSE DATA PROTECTION ACT (1970)

1.1 ORIGIN AND DEVELOPMENT

223. A TALE OF HOPE AND DISENCHANTMENT – Following the "Great Hessen plan" of 1965, the German Federal State ("*Land*") of Hesse embarked upon a large-scale data collection exercise. The goal of this exercise was to assist the government in its development of long-term policies in economic and social matters, such as finance and social security.[454] In 1969, the government enacted legislation which authorized the creation of an integrated data processing system for state and communal data.[455] By

[451] Hesse Data Protection Act of 7 October 1970 ["*Hessen Datenschutzgesetz vom 7. Oktober 1970*"] , *Gesetz- und Verordnungsblatt für das Land Hessen* (HE GVBI), 12 October 1970, nr. 41, Part I, p. 625-627, accessible at http://starweb.hessen.de/starweb/LIS/gvbl.htm (last accessed 18 March 2013).
[452] Swedish Data Act of 11 May 1973 ["*Datalagen*"], SFS 1973: 289.
[453] Law n° 78-17 of 6 January 1978 concerning informatics, files and liberties ["*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, au fichiers et aux libertés*"], Official Journal of the French Republic 7 January 1978, p. 227-231. (corr. 25 January 1978), available at http://www.legifrance.gouv.fr.
[454] S. Simitis, "Privacy – An Endless Debate?", *California Law Review* 2010, Vol. 98, p. 1995. See also S. Simitis, "Zwanzig Jahre Datenschutz in Hessen – eine kritische Bilanz", in Hessischer Landtag, *Neunzehnter Tätighkeitsbericht des hessischen Datenshutzbeauftragten*, 1990, Drucksache 12/7651, p. 68-75, available at http://www.thm.de/zaftda/tb-bfdi/doc_download/421-19-tb-lfd-hessen-1990-127951-vom-11021991 (last accessed 14 March 2013).
[455] A. Newman, *Protectors of Privacy: Regulating personal data in a global economy*, 2008, Cornell University, New York, p. 46. See also Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, 1972, Drucksache 7/1495, p. 8, available at http://www.thm.de/zaftda/tb-bundeslaender/doc_download/448-01-tb-lfd-hessen-197172-71495-vom-29031972 (last accessed 15 March 2013). The law in question was the Law of 16 December 1969 establishing the data processing centre of the State of Hesse and regarding the data processing centres of local communities ["*Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung (HZD) und Kommunaler Gebietsrechenzentren (KGRZ)*"], *HE GVBI*, 22 December 1969, Nr. 32, Part I, p. 304-307, accessible at

using automated data processing techniques, policy makers would be able to "*replace the most intuitive political decisions by rational conclusions based on knowledge of all the relevant data*".[456] Towards the end of the '60s, however, euphoria regarding the benefits of automation started to dwindle, as critical reflections regarding the consequences of such automation began to increase.[457] Two concerns in particular permeated the debate: destabilization of the balance of powers ("*Gewaltenteilung*") and the loss of privacy ("*Verlust jeglicher Privatheit*").[458]

224. UPSETTING THE BALANCE – A first area of concern related to the balance of power between the legislature and the executive. Some worried that the use of automated data processing techniques would unduly strengthen the power of the executive vis-à-vis the legislative branch (by providing the former with an "informational advantage" over the latter).[459] A second set of concerns revolved around the relationship between the State and its citizens. The involvement of nearly all Hesse citizens, combined with the sensitive nature of the data being stored, as well as the databank's capacity to exploit information for different purposes, increased the demands for a public investigation.[460]

225. HISTORY IN THE MAKING – After drawing inspiration from a series of (mainly U.S.) congressional reports and the then burgeoning privacy literature, a draft bill was prepared.[461] On 30 September 1970, the Hessian parliament adopted[462] the world's first data protection act.[463] This Act was the first separate law laying down rules of general application for data protection (i.e. not merely a part of a law by which a data centre was established).[464] As will become apparent over the following sections and paragraphs, the

---

http://starweb.hessen.de/starweb/LIS/gvbl.htm (last accessed 18 March 2013). See also H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 45. As the title suggests, the law also provided a legal basis for the creation of data processing centres at the level of the local communities, which would be under an obligation to co-operate with the State data processing centre (see section 18).

[456] S. Simitis, "Zwanzig Jahre Datenschutz in Hessen – eine kritische Bilanz", *l.c.*, p. 69, citing Minister-President Oswald's preface to the Great Hessen plan (own translation).

[457] *Id.* See also S. Simitis, "Datenschutz", in H. Meyer and M. Stolleis (eds.), *Staats- und Verwaltungsrecht für Hessen*, 1996, fourth edition, Nomos Verlagsgesellschaft, Baden-Baden, p. 110-111.

[458] *Ibid*, p. 69-70. See also Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, 8 July 1970, 6. Wahlperiode (1966-1970), p. 4057-4063, accessible at http://starweb.hessen.de/starweb/LIS/plenarprotokolle.htm (last accessed 20 March 2013).

[459] S. Simitis, "Zwanzig Jahre Datenschutz in Hessen – eine kritische Bilanz", *l.c.*, p. 70 and F.W. Hondius, Emerging data protection in Europe, *o.c.*, p. 5.

[460] S. Simitis, "Privacy – An Endless Debate?", *l.c.*, p. 1995.

[461] *Id.*

[462] Hessischer Landtag, *Plenarprotokolle der 80. Sitzung*, 30 September 1970, 6. Wahlperiode (1966-1970), p. 4271-4272, accessible at http://starweb.hessen.de/starweb/LIS/plenarprotokolle.htm (last accessed 20 March 2013).

[463] S. Simitis, "Privacy – An Endless Debate?", *l.c.*, p. 1995. (noting 10 October 1970 as the date of parliamentary adoption; which appears to be a typographical error)

[464] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 35; M. D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy, *l.c.*, p. 39. Clauses to protect the confidentiality of personal information had already been introduced in the form of administrative regulations to one of the organisational laws seeking to implement data processing public administration, namely the law of 2 April 1968 of Schleswig Hollstein. (H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 45.)

basic tenets of this law would influence the future development of data protection legislation in Europe for decades to come.[465]

1.2 SCOPE

226. PUBLIC SECTOR – The scope of the law was limited to data which was being handled by (or on behalf of[466]) public sector bodies of the State of Hesse. More specifically, the Hessian Act applied to

> "*all records prepared for the purposes of automatic data processing, all stored data and the results of processing such records and data within the purview of the State authorities and the public corporations institutions and establishments under the jurisdiction of the State*".[467]

227. AUTOMATIC PROCESSING – The Hessian Act applied to all forms of automatic processing.[468] The Act also applied to the "input" and "output" of automated processing activities, insofar as the records or data concerned had either been prepared for the purposes of automatic processing or had undergone such processing.[469]

228. (NON-)PERSONAL DATA – From a contemporary perspective, it is interesting to note that the Hesse Data Protection Act did not limit its scope to personal data.[470] As a result, the requirements of the Act in principle applied to all types of data, regardless of whether such data related to a natural person or not.[471] Section 5 of the Act did, however, authorize the communication and publication of data "containing no individual details concerning natural or legal persons permitting and no such details to be inferred" (provided there was no legal prohibition or important public interest preventing it).

---

[465] Section 1 of the Hessian Data Protection Act. See also H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 46.

[466] See Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 11 (stating that the requirements contained in the Act would also apply in cases where a public entity commissioned a private entrepreneur to process data on its behalf). See also *infra*; nr. 121. It is worth noting that the regulation of private enterprises was only debated after the adoption of the Hesse law, seeing as the competence towards private sector activities was (and is) reserved to the Federal Government.

[467] The citations of the Hessian Data Protection Act included in this chapter have been taken from the translation found in U. Dammann, O. Mallmann and S. Simitis (eds.), *Data Protection Legislation. An International Documentation. English – German*, 1977, Alfred Metzner Verlag GmbH, Frankfurt am Main, p. 113-119.

[468] Limiting the scope to electronic data processing would have allegedly constituted a discrimination towards computers. (H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 47.)

[469] See also Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 22.

[470] The Hesse Data Protection Act sought to prevent unauthorized access to government data files in general. See Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, *l.c.*, p. 4057.

[471] See also *ibid*, p. 27.

1.3 BASIC PROTECTIONS

229. OVERVIEW – The Hesse Data Protection Act had essentially three objectives: (1) to prevent unauthorized access to government data files; (2) to protect individuals against the potential dangers of automated data processing and (3) to secure the legislature's access to information.[472] The Act also provided for institutional control by creating a Data Protection Commissioner's office which would be tasked with oversight.[473]

A. Protection of data

230. SECURITY AND CONFIDENTIALITY – Section 2 of the Hessian Data Protection Act provided that all records, data and results covered by its scope

> "*shall be obtained, transmitted and stored in such a way that they cannot be consulted, altered, extracted or destroyed by unauthorized persons*".[474]

This provision essentially obliged the relevant public authorities to ensure the security of the data being processed through appropriate technical and organisational measures. Section 3(1) goes on to state that the persons charged with the handling of data "shall be prohibited from communicating or making available to other persons the records, data and results gained during the course of their duties and from enabling other persons to obtain such information", except where this is authorized by law or by the consent of "those entitled to exercise control"[475] over the records, data and results.

B. Rights for individuals

231. CLAIM TO DATA PROTECTION – Section 4 of the Hessian Data Protection Act introduced two rights, namely (1) a right to rectification and (2) a right of "blocking". The former enabled any aggrieved party to demand the rectification of incorrect data (section 4(1)). The latter enabled any person whose rights were infringed by unlawful access, alteration, destruction or extraction, to demand that such action be discontinued if there was a danger of further infringement (section 4(2)). In addition to these two specific rights, section 11 also introduced a general right of complaint to the Data Protection Commissioner for anyone who considered that his or her rights had been infringed by automated data processing.

---

[472] Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, *l.c.*, p. 4057; Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 18 (intervention by S. Simitis).

[473] See also F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 35.

[474] See also section 5(2) which imposed access control restriction in the case of data banks and information systems.

[475] Cf. *infra*; nr. 241.

C. Access to information by legislature

232. RIGHT TO INFORMATION – One of the main objectives of the Hessian Act was to secure the legislature's access to information. To this end, section 6 of the Act obliged the administrative bodies who operated data processing centres[476] to provide the State legislature and its parliamentary parties any information they requested from the stored data.[477] The same right was also provided to the district and local councils, their political groups, as well as other public bodies, each within their sphere of responsibility (section 6(2)).[478] If a request for information was not met or fully satisfied, each beneficiary could require the Data Protection Commissioner to investigate the matter (section 12).

D. Data Protection Commissioner

233. MISSION – In order to promote the effective implementation of its rules, the Hessian Data Protection Act created a Data Protection Commissioner's office. This entity had the responsibility of ensuring that all public sector entities which fell within the scope of the act acted in compliance with its provisions. Its mission also extended to other regulations governing the confidential handling of information provided by citizens and of records relating to individual citizens (section 10(1)). In addition, the Data Protection Commissioner was charged with monitoring the effects of automatic data processing on the operation and powers of the public sector entities that fell within the scope of the Act and to note whenever there was (risk of) displacement in the distribution of powers (section 10(2)).

234. POWERS – In case of infringement, the Data Protection Commissioner was required to inform the responsible supervisory authorities ("*Aufsichtsbehörde*") and to suggest appropriate measures to improve data protection (section 10(1) and 10(2)). All public sector bodies falling within the scope of the Act were required to provide the Data Protection Commissioner with the information he needed in the performance of his duties (section 13). Each year, the Data Protection Commissioner would be required to submit an annual report documenting the results of his activity to the State Parliament and the Prime Minister (section 14).[479]

---

[476] More specifically, this provision of the Act refers to the Hesse data processing centre, the local district computer centres and the State authorities operating data processing installations.

[477] This general right to information was subject to 4 conditions: (1) the request was within the jurisdiction of that entity ["*im Rahmen ihrer Zuständigkeiten*"]; (2) the information in question did not contain details concerning natural or legal persons and permitted no such details to be inferred; (3) there was no legal prohibition against it and (4) no important public interest to prevent it.

[478] The scope of this right was slightly different than that of the State parliament, in that it referred to "relevant" local district computer centres and other data processing operated by the municipalities and counties (compare *supra*; footnote 476).

[479] The annual reports of the Hessen DPA can be accessed at http://www.thm.de/zaftda/tb-bundeslaender/cat_view/25-tb-bundeslaender/12-hessen/22-landesdatenschutzbeauftragter (last accessed 18 March 2013).

1.4 ALLOCATION OF RESPONSIBILITY AND RISK

235. ABSENCE OF GENERAL CRITERIA – The Hesse Data Protection Act did not explicitly define which actors (or types of actors) would be responsible for ensuring compliance with its provisions, at least not within the scope section of the law. Section 1 did include a reference to "*Land authorities and public corporations, institutions and establishments*" in defining the scope *ratione materiae* (cf. *supra*; nr. 226); but provided no general criteria[480] to determine which of these entities would be deemed responsible for the actual implementation of data protection measures in a specific instance.

236. CONFERRED AUTHORITY – One possible explanation for the absence of general criteria relates to the context in which this Act would be applied. Seeing as the scope of the Act was limited to data processing carried out by (or on behalf of) public sector bodies, the activities would be governed by the general principles of public law. As a rule, the activities of public sector bodies require a basis in law in order for them to be legitimate. Data processing may therefore in principle only be undertaken if there is a legal basis authorizing it.[481] If one expects that to be the case, one might have also considered it unnecessary at that time to include further criteria, as the roles and responsibilities of each actor would be ascertainable from the relevant legislation.[482]

237. SPECIFIC RESPONSIBILITIES – While the Hesse Data Protection Act did not use any general criteria to allocate responsibility, several of its provisions were targeted at specific entities. In particular, references can be found to "responsible persons" ("*betrauten Personen*")[483], the "supervisory authority" ("*die Aufsichtsbehörde*")[484] and "those entitled to exercise control" ("*derjenigen die verfügungsberechtigt sind*")[485].

---

[480] By "general criteria" I mean to refer to criteria of general application, i.e. a standard, rule or test on which a decision can be based and which can be applied in a wide variety of instances.

[481] This principle was later explicitly codified in the Hessian Data Protection Act of 31 January 1978 (*HE GVBl.* 7 February 1978, nr. 4, I, p. 96), specifically in section 7. See also S. Simitis, "Datenschutz", *l.c.*, p. 125 ("*Ohne gesetzliche Grundlage dürfen die öffentlichen Stellen keine personenbezogene Daten verwenden.*")

[482] This explanation was proffered to me by Spiros Simitis in the course of an email exchange which took place in March 2013. Specifically, Prof. Simitis explained to me that: "*It is correct [reference to what is currently paragraph 60] that the Hesse law did not explicitly indicate criteria. But there was a clear reason. Each entity has specific tasks. And it is precisely these tasks that not only legitimate the existence of a particular entity, but also define the legally acceptable choice of the data to be processed. The Hesse Act was nonetheless linked to the expectation that a growing consciousness of the importance of data protection would also support the efforts to precisely name the purposes of the various entities and thus avoid the risks of an enlarging expansion of their activities.*"

[483] See section 3(1).

[484] See section 6(1). From a contemporary perspective, it is also interesting to note that this term has also been translated in the past as "the *controlling* authority", e.g. in the translation found in U. Dammann, O. Mallmann and S. Simitis (eds.), *Data Protection Legislation. An International Documentation. English – German*, 1977, Alfred Metzner Verlag GmbH, Frankfurt am Main, p. 113-119 (which was an unofficial translation made by the OECD, Informatics Studies No. 2, 1971, p. 47) .

[485] See section 3(1) ("*derjenigen die verfügungsberechtigt sind*" can also be translated as: "*those authorized to dispose of*").

238. RESPONSIBLE PERSONS – It is reasonable to infer that the term "responsible persons" ("*betrauten Personen*"), as it is used in section 3 of the Act, was intended to refer to the administrative staff who were engaged in the actual handling of data. This inference is supported both by the language of this provision as well as the fact that the duty contained in this provision was considered to be complementary to the general duty of confidentiality incumbent upon public servants.[486]

239. OPERATORS OF DATA PROCESSING CENTRES – The Hesse Data Protection Act also addressed the administrative bodies who were in charge of operating the data processing centres.[487] In particular, section 6 of the Act obliged these entities to provide the legislative (and associated) bodies with any information they requested from the stored data, provided this request resided within their sphere of responsibility.[488] In addition, even though this was not spelt out explicitly in the Act, compliance with data protection was also deemed to be an essential component of their administrative task.[489]

240. SUPERVISORY AUTHORITY – The term "supervisory authority" ("*Aufsichtsbehörde*") appeared twice in the Hessian Data Protection Act, namely in section 6(3) and section 10(1).[490] While the term "supervisory authority" was not defined within this Act, it previously appeared in the Law of 16 December 1969 establishing the data processing centre of the State of Hesse and regarding the data processing centres of local communities.[491] As the Hessian Data Protection Act was regarded as a follow-up to the aforementioned law[492], it is reasonable to assume that this term was intended to have a similar meaning within both laws.[493] The term "*Aufsichtsbehörde*" should not, however, be confined to any particular supervisory authority. This term is used as a general reference for any government office exercising supervisory authority and especially control functions. Any reference to the

---

[486] See Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, 8 Juli 1970, 6. Wahlperiode (1966-1970), p. 4057.

[487] More specifically, section 6(1) of the Act refers to the Hesse data processing centre, the local district computer centres and the State authorities operating data processing installations.

[488] Cf. *supra*; nr. 117.

[489] See Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 24: "*The Hessian Data Processing Centre and the Data Processing Centres of the local communities process data as a service; it is the purpose of their establishment, not a tool supporting their activities. Hence data protection is an essential component of their administrative task, both in terms of the protection of personality ["persönlichkeitsschutzes"] as well as in terms of data security*".

[490] Section 6(3), which deals with the Legislature's right of access, specifies that "*in case of doubt the decision of the supervisory authority shall be final*" (referring to instances in which there may be a disagreement as to whether or not a particular legislative body should in fact be provided with access). Section 10(1) deals with the duties and powers of the Data Protection Authority. It provides that the Data Protection Commissioner "*shall inform the responsible supervisory authorities of any infringements committed and shall suggest appropriate measures to improve data protection*".

[491] Cf. *supra*; footnote 455.

[492] See Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, 8 Juli 1970, 6. Wahlperiode (1966-1970), p. 4057. See also H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 45.

[493] Section 14 of the Law of 16 December 1969 identified the Hessian Prime Minister as the "supervisory authority" of the data processing centre of the State of Hesse. Section 21 of the same law assigned the Hessian Minister of Interior the task of supervising the data processing centres of the local communities.

"responsible" supervisory authority must be therefore understood in the context of the activities at issue.[494]

241. THOSE ENTITLED TO EXERCISE CONTROL – Section 3(1) provides that persons charged with the handling of data may only share such data with others when this is authorized either by law or by the consent of "those entitled to exercise control" ("*derjenigen die verfügungsberechtigt sind*").[495] In his first annual report, the Data Protection Commissioner highlighted some of the difficulties arising from the fact that the Hesse Data Protection Act did not specify who would be authorized to decide over the disclosure of data (or under which conditions).[496] The Data Protection Commissioner did not, however, advocate for a statutory definition of these actors. Instead, he recommended that, in particular where intimate data were concerned, administrative arrangements be put in place to ensure that the decision is made by either the head of the "issuing authority" ("*abgebenden Behörde*") or an especially designated civil servant ("*besonderes verpflichteter Bediensteter*").[497]

242. ISSUING AUTHORITY – It stands to reason that the terms "issuing authority" ("*abgebenden Behörde*") (which can also be translated as: "leaving" or "submitting" authority) in first instance referred to the public bodies who had requested the processing of certain data to support the exercise of their official duties. Section 5 of the Law of 16 December 1969 provided that every member or customer of the State data processing centre had a right to access its own data file. This language, together with language used by the Data Protection Commissioner in his first annual report, suggests that the term "issuing authority" referred to those entities who had entrusted the processing of data to either a State or local processing centre (thereby effectively "leaving" or "submitting" the data with (to) the processing centre).

243. A SHARED RESPONSIBILITY – Based on the foregoing considerations, one can conclude that the responsibility for ensuring compliance with the Hesse Data Protection Act was shared, at least in part, by all entities involved in the preparation and execution of automatic data processing. Four sets of actors in particular are targeted by the law: (1) the administrative staff engaged in the actual handling of data; (2) the operators of

---

[494] This explanation was proffered to me by Spiros Simitis in the course of an email exchange which took place in April 2013. Specifically, Prof. Simitis explained to me that: ""*Aufsichtsbehörde" is a term generally used for Government offices exercising supervisory and especially control functions. Their specific tasks and duties can consequently only be indicated as long as the particular context of their activities is considered. The references to the "Aufsichtsbehörden" in sections 6(3) and 10(1) must be read and understood in precisely this sense.*"

[495] Cf. *supra*; nr. 230.

[496] See Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 25-26.

[497] *Ibid*, p. 33. In subsequent annual reports, however, the Data Protection Commissioner did call for a statutory definition of criteria to determine when the disclosure of data should be deemed permissible. See e.g. Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Vierten Tätighkeitsbericht*, 1975, Drucksache 8/438, p. 8.

the data processing centres[498]; (3) the public authorities who requested data processing to take place; and (4) the relevant supervisory authorities. The fact that data protection was considered part of the statutory duty of the operators of the data centres is an indication that that those engaged in the actual processing operations were considered responsible for implementing appropriate data protection measures.[499] At the same time, the reference to "those entitled to exercise control" in section 3 suggests that the decision-making power over the disclosure of data (and the responsibility to exercise this power appropriately) may lie elsewhere than with the actual holders of the data.

244. OUTSOURCING – The Hesse Data Protection Act also applied in situations where a public authority commissioned a private entrepreneur to process data on its behalf.[500] The Data Protection Commissioner emphasized that in such cases the public authorities concerned with the automatic data processing remain responsible and accountable for the implementation of appropriate data protection measures.[501] He also indicated that, in case of co-operation with private entities, additional security measures might be necessary. Specifically, the public sector entities concerned were responsible for ensuring that an equivalent level of protection is maintained at all times.[502]

245. RISK – Section 16 of the Hesse Data Protection Act provided that it shall be an offence of any person to, either intentionally or through negligent participation, provide an unauthorized person with access to information protected by the Act in violation of Section 3.[503] The Hesse Data Protection Act does not make reference to any other liabilities or sanctions in case of non-compliance. While Section 3 mainly targets the administrative staff who were tasked with handling the data ("*betrauten personen*"), one can nevertheless assume that the authorities in charge of the data processing centres and/or the public authorities who were requesting data processing to take place might be held accountable (or even liable) in case of failure to implement appropriate data

---

[498] See also F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, at p. 35: "[The Hessian Data Protection Act] lays down norms on data confidentiality *which should observed by the authorities in charge of data processing and computer personnel*".

[499] See also Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 24 ("*The Hessian Data Processing Centre and the Data Processing Centres of the local communities process data as a service; it is the purpose of their establishment, not a tool supporting their activities. Hence data protection is an essential component of their administrative task, both in terms of the protection of personality ["persönlichkeitsschutzes"] as well as in terms of data security*").

[500] Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 11.

[501] *Ibid*, at p. 33 ("*Verantwortlichkeit der Verwaltungen - Entgegen manchen Äusserungen und Erwartungen ist daran zu erinnern, dass die volle verantwortung für die Durchführen des Datenschutzes den Behörden und Stellen obliegt, die mit der maschinellen Datenverarbeitung befasst sind*")

[502] *Id.*

[503] This provision was modified by the Law of 4 September 1974 (*HE GVBl.* 9 sept. 1974, nr. 27, I, p. 365) to stipulate that such offences may be punished by imprisonment up to one year or by a fine. The same penalty would apply if this person collaborated with another person who improperly obtained access to information or if the responsible person made improper use of the information. If the offender were acting for consideration or with the intention of obtaining financial benefit for himself or for another, or of harming another person, the penalty could be increased to two years (section 16(2)).

protection measures, particularly where this failure falls short of a reasonable standard of care.

1.5 CONCLUSION

246. EXPERIMENTAL NATURE – The Hesse Data Protection Act has been characterized as "trial and error" legislation: a considerable portion of the law focused on the establishment of a Data Protection Commissioner, who would watch over the application of the law and gather experience.[504] By defining the Commissioner's role in broad terms, the Act allowed for continuous adjustment to the progressively increasing automation of public administration.[505]

247. A SOURCE OF INSPIRATION – While the level of detail may have been limited, the Hessian Act contained several elements which would influence data protection legislation for decades to come.[506] First, the Act put in place a default confidentiality rule for data processing: in principle, all data undergoing automated processing should be kept confidential, unless there was an explicit authorization to disclose.[507] The Act also attributed rights to individuals who might be affected by the processing, in particular the right to rectification and the right of "blocking".[508] A third element of influence was the establishment of institutional oversight.[509] While the powers of supervisory bodies would vary from country to country, the basic notion of charging a governmental entity with oversight of data protection rules was echoed in data protection laws throughout Europe.

248. ALLOCATION OF RESPONSIBILITY AND RISK – The 1970 Hesse Data Protection Act did not formally define how responsible entities should be identified. However, a number of its terms, such as "those entitled to exercise control" and "data processing centres", display both a conceptual and linguistic similarity with the terms "controller" and "processor" later adopted by Directive 95/46/EC. In addition, the first annual reports of the Hessian Data Protection Commissioner identified a number of issues which would become recurring themes in subsequent discourse, such as the need for additional measures when entrusting data processing to other entities who are not directly subject to the act.

---

[504] H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 46.
[505] See Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 12 ("*[…] the Data Protection Act defines the scope of the mission of Data Protection Commissioner in broad terms and allows for the adjustment to the progressively increasing automation of public administration and the development of the techniques of data processing*") (own translation).
[506] H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 46.
[507] *Ibid*, p. 45.
[508] Cf. *supra*; nr. 231.
[509] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 35; H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 46

249. AFTERMATH – The Hesse Data Protection Act has been revised a total of four times since its initial enactment in 1970. The first revision, introduced in 1978, was relatively minor.[510] The second revision took place in 1978, shortly after the adoption of the federal data protection law of Germany ("*Bundesdatenschutzgesetz*").[511] A third revision was made in 1986, after the decision of the German Constitutional Court in the census case ("*Volkzählungsurteil*").[512] Finally, a fourth set of revisions was introduced in 1998 to bring the Act in compliance with EU Directive 95/46/EC.[513]

[510] The Law of 4 September 1974 (*HE GVBl.* 9 September 1974, nr. 27, I, p. 365) modified section 16 of the Act to stipulate that violations of the Act may be punished by imprisonment up to one year or by a fine. If the offender were acting for consideration or with the intention of obtaining financial benefit for himself or for another, or of harming another person, the penalty could be increased to two years (cf. *supra*; footnote 503).

[511] Law of 31 January 1978, *HE GVBl.* 7 February 1978, nr. 4, I, p. 96. The revision of the Hessian Act did not merely serve to bring it in compliance with the federal act, however, it also introduced a number of new elements and precisions. (S. Simitis, "Datenschutz", *l.c.*, p. 112; S. Simitis (ed.), *Kommentar zum Bundesdatenschutzgesetz*, 2003, Baden-Baden, Nomos Verlagsgesellschaft, 5th edition, p. 2-3).

[512] Law of 11 November 1986, *HE GVBl.* 20 November 1986, nr. 25, I, p. 309. This is the decision in which the German Constitutional Court famously recognized the citizen's right to informational self-determination ("*informationelle Selbstbestimmung*") (Bundesverfassungsgericht, Decision of 15 December 1983 regarding Volkzählungsgesetz 83, *BVerfGE* (Entscheidungen des Bundesverfassungsgerichts) vol. 65, p. 1 et seq. For more information regarding the census case see S. Simitis (ed.), *Kommentar zum Bundesdatenschutzgesetz*, *o.c.*, p. 14 et seq. For more information regarding the third set of revisions to the Hessian Data Protection Act see S. Simitis, "Datenschutz", *l.c.*, p. 112-116.

[513] Law of 5 November 1998, *HE GVBl.* 9 November 1998, nr. 22, I, p. 421.

2 THE SWEDISH DATA ACT (1973)

2.1 ORIGIN AND DEVELOPMENT

250. EARLY ADOPTERS – In comparison to other countries, Sweden was relatively early in achieving widespread adoption of computers.[514] In the beginning of 1960's, the Swedish government began to expand its use of automated data processing ("ADP") within the public sector significantly.[515] It developed a comprehensive system of centralized data banks, which progressively became operational starting in 1963.[516] At first, this "computerization" of public administration was largely perceived as a rational and positive development.[517] Towards the end of the 60's, however, general perception had become less equivocal.[518] The ensuing political debate centred around two core issues: transparency and privacy.

251. A TRADITION OF OPEN GOVERNMENT – Many commentators attribute Sweden's early adoption of data protection legislation – at least partially – to its unique tradition of openness and transparency.[519] For more than two centuries, Sweden has recognized a general principle of free access to all public documents.[520] Pursuant to this principle, everyone has a right to view all official documents and request a copy.[521] Any exception

---

[514] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 62. See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, & the United* States, 1989, Chapel Hill, The University of North Carolina Press, p. 96.

[515] See L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *HUMAN IT* 2007, Vol. 9, No. 1, p. 9.

[516] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 44. Prominent examples included the population registry, motor vehicle registration, register of business firms, land records, police files, social service and employment offices. (*Id.*) See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 96 (characterizing Sweden as "a paradise for registers").

[517] L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 9.

[518] *Ibid*, p. 9-10.

[519] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 62. See also R. Pagano, "Panorama of Personal Data Protection Laws", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 305 and D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 94.

[520] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 305 ("public documents" in this context comprise all documents transmitted to public bodies or drawn up by them). (*Id.*) This "publicity principle" was first codified in 1766 by way of an Ordinance Relating to the Freedom of Writing and the Press (see J. Mustonen (ed.), *The World's First Freedom of Information Act. Anders Chydenius' Legacy Today*, Anders Chydenius Foundation's Publications 2, 2006, available at http://www.access-info.org/documents/Access_Docs/Thinking/Get_Connected/worlds_first_foia.pdf (last accessed 1 August 2013.) This publicity principle was later reaffirmed in the Freedom of the Press Act of 1949, which is one of the four basic laws of the Swedish constitution. For purposes of completeness, we must note that the principle of publicity was suspended several times during this time period.

[521] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 305. This principle can only be limited by specific legislation. (*Id.*) See also C.G. Källner, "Personal Data: The Open Access Approach", in OECD, *Policy issues in data protection and privacy*. *Concepts and perspectives*, Proceedings of the OECD Seminar 24th-26th June 1974, OECD Informatics Studies, no. 10, 1976, Paris, p. 59-60 and J. Freese, "The Swedish

to this principle must be established by law and is construed narrowly.[522] As the use of computers became more widespread, fears arose that this might threaten the public's ability to exercise their rights of access.[523] Specifically, there was a concern that members of the public, who could find their own way through a manual file, would experience difficulties in the face of an electronic register.[524]

252. TOO MUCH OF A GOOD THING … – A second set of concerns, somewhat contradictory to the former, related to the privacy of individuals.[525] The computerization of public records, in combination with the principle of publicity, was making it possible for private actors to obtain massive amounts of information on individuals.[526] Among these private actors were also commercial enterprises, such as credit agencies and advertising agencies.[527] Moreover, the ability to link information about specific individuals was facilitated considerably by the fact that the Swedish government employed a highly developed system of personal identification numbers.[528] Given the comprehensive nature of Sweden's public sector data banks, fears grew that these developments would upset the existing social equilibrium and result in invasion of individuals' privacy.[529]

Data Act", *Current Sweden* 1977, No. 178, p. 1, available at https://www.ncjrs.gov/pdffiles1/Digitization/49670NCJRS.pdf (last accessed 2 August 2013) (noting that it was "*[…] very easy to take advantage of this right. Anyone can visit the offices of government agencies and ask to look at their documents*"). (*Id.*)

[522] J. Freese, "The Swedish Data Act", *l.c.*, p. 1. The so-called "Secrecy Act" ("Sekreteslag") of 28 May 1937 provided the legislative basis for exceptions to the general principle of publicity (*Id.*).

[523] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 63.

[524] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46. Even though the public's right of access extended to computerized records, there was still the concern that members of the public might require special computer facilities or aid of specialized personnel to enable them to exercise their right of access. (*Id.*)

[525] *Id.*

[526] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 63. See also C.G. Källner, "Personal Data: The Open Access Approach", *l.c.*, p. 59-60.

[527] *Id.* See also L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 22 (describing a case involving the commercial use of local housing authorities records which triggered initiated the discussion of the privacy problem at the level of the Riksdag in December 1967).

[528] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 62 and D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 94 and 98 (noting that the use of national identification numbers as the standard identifier for individuals in a public and private information systems facilitates the linkage of information, which can lead to surveillance and/or abusive personality profiling).

[529] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46. The population and housing and housing census of 1970 is said to have been the "spark" that set off the privacy debate in earnest: see L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 13-16. See also P.G. Vinge, *Swedish Data Act*, Federation of Swedish Industries, No. 43, Svanbäck & Nymans Boktr., Stockholm, 1974 (original release: 1973), p. 6 (signalling an exceptional high number of complaints occasioned by the 1970 Census).

253. COMMITTEE ON PUBLICITY AND SECRECY – As time passed, the call for a governmental investigation into the balance between openness and privacy grew.[530] In April 1969, the Swedish government set up the Committee on Publicity and Secrecy Legislation ("*Offentlighets och Sekretesslagstifningskommiten*" - OSK).[531] This multi-stakeholder expert group was asked to prepare legislation on the publicity and secrecy of public documents in light of electronic processing techniques.[532] While the Committee initially focused on the publicity issue (i.e. how could the principle of public access be extended to computer media), privacy issues came to the fore during the latter part of 1970.[533] In 1972, after having carried out a number of inquiries, consultations and hearings, the OSK presented its report, entitled "*Data and Integrity*" ("*Data och integritet*"), which proposed a number of legislative amendments.[534]

254. LEGISLATIVE PROPOSALS – With regard to the publicity issue, the OSK proposed an amendment to the Freedom of the Press Act.[535] This amendment would ensure that the rules applicable to paper documents would also apply to computer media and other technical recordings; with specific rules on the handing out of such recordings.[536] With regard to the issue of privacy protection, the OSK proposed an all-new "Data Act" ("*Datalag*"), which would essentially subject the creation of computerized records containing personal information to prior approval.[537]

255. THE FIRST NATIONAL DATA PROTECTION ACT – The proposed Data Act was formally adopted on 11 May 1973.[538] The Swedish Data Act[539] represented the first

---

[530] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 63.

[531] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 306; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 63 and L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 23. The so-called "Secrecy Act" ("Sekreteslag") of 28 May 1937 provided exceptions to the general principle of publicity (F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 45). This Act had for long time governed access to sensitive data, including the results of population and housing censuses. However, many felt that these regulations were insufficient in an increasingly computerized society. (L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 14)

[532] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 306.

[533] L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 24. As indicated earlier, the population and housing and housing census of 1970 is said to have been the "spark" that set off the privacy debate in earnest (cf. *supra*; footnote 529). See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 63.

[534] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 306-307.

[535] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46.

[536] L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 25. See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 7.

[537] *Id.*

[538] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46.

[539] Data Act (Datalagen), SFS 1973: 289. An English translation can be found in U. Dammann, O. Mallmann and S. Simitis (eds.), *Data Protection Legislation. An International Documentation. English – German*, *o.c.*, p. 129-145 and in OECD, *Policy issues in data protection* and privacy, o.c., p. 298-305.

piece of data protection legislation adopted at national level.[540] It came into (partial) force on 1 July 1973.[541]

2.2 SCOPE

256. PUBLIC AND PRIVATE SECTOR – Because of the principle of free access to public records, the Swedish government felt the need to address the private and public sector in conjunction with one and other.[542] The Swedish Data Act was therefore equally applicable to both public and private sector data processing.[543]

257. PERSONAL REGISTERS – The Act applied to "personal registers", which were defined in Section 1 as "*any register or other notes made by automatic data processing and containing personal information that can be assigned to the individual concerned*".[544] The Swedish Data Act thus only applied to *automatic* data processing which involved personal information (not to manual records).[545]

258. PERSONAL INFORMATION – "Personal information" was defined in the Act as "information concerning an individual" (section 1). Hence property registers or motor vehicle registers were also covered if they contained information by which the owners could be identified.[546] A "registered individual" was in turn defined as "*an individual in respect of whom personal information occurs in a register*" (section 1).

---

[540] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 44; R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 305; M. D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy, *l.c.*, p. 39; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 60; H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 48 and L. Ilshammar, "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *l.c.*, p. 26.

[541] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 307. The entirety of its provision came into force on 1 July 1974, after the amendment of the Freedom of the Press Act was completed. See also J. Freese, "The Swedish Data Act", *l.c.*, p. 1; P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 18-19.

[542] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 46 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 161.

[543] J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 161; M. D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy, *l.c.*, p. 39 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 161.

[544] The citations of the Swedish Data Act included in this chapter have been taken from the translation found in U. Dammann, O. Mallmann and S. Simitis (eds.), *Data Protection Legislation. An International Documentation. English – German*, *o.c.*, p. 129-145.

[545] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 161. See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 104.

[546] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 161. See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9 and J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 159.

2.3 BASIC PROTECTIONS

259. OUTLINE – The Swedish Data Act sought to protect individuals' privacy by subjecting the creation of personal registers to prior approval and regulation and by imposing a number of duties upon the "responsible keeper" of a register. It also established a Data Inspection Board (DIB) endowed with broad supervisory powers.

A. Prior authorization

260. CONTROLLING THE COMPUTER – Section 2 of the Swedish Data Act provided that "*no personal register may be started or kept without permission by the Data Inspection Board*". The rationale behind this provision was to prevent the creation of new registers which unduly interfered in individuals' privacy.[547] By doing so, the Act sought to protect privacy without detracting from the open access principle: all publicly held information would remain accessible as it was before, whereas the automated processing of this information could be regulated to protect privacy.[548]

261. A COMPREHENSIVE LICENSING SCHEME – In principle, all automatic processing of personal information was subject to prior approval by the Data Inspection Board (DIB). A basic premise underlying the Data Act had been that "*all information about the conditions of individuals may concern privacy*".[549] As a result, any computerization of personal information in principle required a license from the DIB. The only exception to this rule were the personal registers established by the King or Parliament (section 2). However, even in those instances the DIB still needed to be heard and had the authority to suggest regulations (see section 7).[550]

262. INTERNATIONAL TRANSFERS – Under section 11 off the Data Act, special permission by the DIB was also required "*if there is reason to believe that personal information will be used for ADP abroad*". This effectively meant that computerized personal information could not be transferred to another country without a specific license issued by the DIB.[551] This restriction applied also in case of transfer to other EU countries.

---

[547] C.G. Källner, "Personal Data: The Open Access Approach", *l.c.*, p. 61-62.
[548] *Id.*
[549] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 64, citing Sweden, Commission on Publicity and Secrecy of Official Documents, *Computers and Privacy* (English translation of the report *Data och Integritet*), Stockholm, Ministry of Justice, 1972, p. 5. See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 11, seemingly citing the same report ("*Even if each item of information may be considered harmless in isolation, the totality of accumulated information may still constitute a serious threat to privacy*")
[550] See also C.G. Källner, "Personal Data: The Open Access Approach", *l.c.*, p. 61. See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 10.
[551] See also M. D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy", *l.c.*, p. 28.

263. ASSESSMENT CRITERIA – The DIB was to grant permission if there was no reason to assume that it would lead to "*undue encroachment on the privacy of individuals*" (section 3, first indent). This assessment was to take into account in particular (1) the kind and quantity of personal information meant to be included in the register and (2) the attitude towards the register shown or expected from the individuals meant to be registered (section 3, second indent).[552]

264. REGISTERS CONTAINING SENSITIVE INFORMATION – For certain types of personal registers, a particularly compelling justification was required if the requestor was someone other than a government agency which had been mandated by law or statute to keep such records.[553] This was for example the case for personal registers containing information about criminal convictions or coercive actions under the Child Welfare Act (see section 4, first indent). Similarly, permission to start and keep a personal register containing information about anybody's political or religious views could only be granted where there were special reasons for this (section 4, first indent).[554]

265. MODALITIES OF LICENSE – When granting a permission, the DIB was to issue specific "regulations" or "directives" which would constrain the license that was given. Certain directives were mandatory, namely directives as to the *purpose of the register* and the personal *information that could be included* (section 4).[555] In addition, the DIB could also, if it considered it necessary to prevent undue encroachment on privacy, issue *additional regulations* (e.g., concerning the technical equipment used, information to be provided to the registered persons, security measures, deletion of personal information etc.) (See section 6, first indent).[556] These regulations were not, however, allowed to restrict the duties of public authorities under the Freedom of the Press Act (section 6, second indent).

266. PRACTICAL DIFFICULTIES – Needless to say, the act of licensing every personal register in Sweden entailed a considerable administrative burden. Quite soon after the Data Act entered into force, the DIB introduced a "simplified procedure" which was used for applications involving "routine" data processing.[557] The simplified procedure, which

---

[552] See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 10 and D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 104-106 (highlighting the vagueness of the criteria "privacy" and "undue encroachment").
[553] J. Freese, "The Swedish Data Act", *l.c.*, p. 3. Section 4, first indent speaks of "extraordinary reasons", whereas section 4 second indent speaks of "special reason". See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 11.
[554] This restriction died not apply to personal registers that an association wanted to keep of its own members (section 4, third indent *in fine*).
[555] J. Freese, "The Swedish Data Act", *l.c.*, p. 3.
[556] See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 12-13.
[557] C.G. Källner, "Personal Data: The Open Access Approach", *l.c.*, p. 63; J. Freese, "The Swedish Data Act", *l.c.*, p. 6 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 164-165. This procedure was applied in cases where a personal data register would not include more information than stipulated on the standardized form and was not going to be used otherwise than granted by the form (*Id.*).

bore greater resemblance to a registration procedure than to a licensing procedure, allowed the DIB to dispose of the majority of applications in summary fashion.[558] This standard operating procedure was later sanctioned by amendments introduced in 1979.[559]

B. Duties of a "responsible keeper"

267. OVERVIEW – Processing of personal information was in first instance regulated by the directives issued by the DIB. As indicated earlier, these directives would at a minimum concern the purpose of the register and the information that could be included.[560] In addition to abiding by these directives, the entity responsible for a personal register (i.e. its "responsible keeper"[561]) needed to observe a number of duties, which were specified in sections 8-14 of the Data Act. These duties concerned *inter alia* (1) the accuracy and completeness of personal information; (2) the right to information of a registered individual; (3) restrictions upon dissemination of personal information and (4) secrecy requirements.[562]

268. CORRECTION – Section 8, first indent of the Data Act provided that

> "*if there is reason to suspect that personal information in a personal register is incorrect, the responsible keeper of the register shall, without delay, take the necessary steps to ascertain the correctness of the information and, if needed, to correct it or exclude it from the register*".

This provision essentially entailed a duty to ensure accuracy of registered information.[563] If a piece of information was corrected or excluded due to its inaccurate nature, the registered individual had the right to demand that the responsible keeper notify any person who had been handed the information in question of its correction or exclusion (section 8, second indent).[564]

---

[558] *Id.*

[559] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 307. A further step was taken with the amendments of 1982, which introduced a formal distinction between "licenses" and "permissions". (*Ibid*, p. 307-308). See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 95 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 165.

[560] Cf. *supra*; nr. 265.

[561] Cf. *infra*; nr. 275

[562] The Swedish Data Act also included specific provisions on the duties of a responsible keeper in case of discontinuance of a register (section 12) and the use of information from an ADP recording for the purpose of judicial or administrative proceedings (section 14).

[563] The extent of this duty of course needed be interpreted within reason. An acceptable level of accuracy should be reached, taking into account the uses of the data. (D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 107). For example, the DIB accepted a lower level of reliability for information used for statistical as opposed to administrative purposes. (*Id.*)

[564] If there were special circumstances the DIB could exempt the responsible keeper from this duty to notify (section 8, second indent *in fine*).

269. SUPPLEMENTATION – If a personal register did not include an item of information that ought to have been included, the responsible keeper was obliged to supplement the register with that which is needed to render it complete (section 9). Whether or not a register needed to be supplemented was determined by taking into account, on the one hand, the purpose of the register and, on the other hand, the risk of "undue encroachment" on individuals' privacy or loss of rights (section 9 *in fine*).[565]

270. RIGHT TO INFORMATION – If a registered person so requested, the responsible keeper was obliged to inform him of the personal information concerning him contained in the register (section 10, first indent).[566] Such information was to be provided free of charge, unless the DIB had permitted otherwise (section 10, second indent). The duty to inform a registered persons did not apply in cases where a law, statute or decision by an authority prohibited the disclosure of this information to the individual concerned (section 10, third indent).

271. RESTRICTIONS UPON DISSEMINATION – Section 11, first indent, provided that personal information contained in a personal register "may not be issued if there is reason to assume that the information will be used for ADP contrary to this act." This meant that personal information should not be disclosed if there was reason to believe that this information might be used to further undue encroachment on personal privacy.[567]

272. SECRECY – A further restriction upon dissemination was stipulated in section 13 of the Swedish Data Act, which provided that "the responsible keeper of a personal register and any other person who has concerned himself with it may not without authorization reveal what he has learnt from it about the personal circumstances of an individual". This provision essentially obliged responsible keepers to observe professional secrecy with respect to what they have found out about private persons in the course of their data processing.[568]

---

[565] See also J. Freese, "The Swedish Data Act", *l.c.*, p. 4. See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 14.
[566] The DIB could also issue a directive which required the responsible keeper to actively notify registered persons of the existence of the register. However, the general rule included in the Data Act itself only provided for a passive information obligation (i.e. upon request). See J. Freese, "The Swedish Data Act", *l.c.*, p. 4.
[567] D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 108. In case of publicly held documents, restrictions were contained in the Act on Restrictions of the Right to obtain public documents (a.k.a. the "Official Secrets Act") (section 11 *in fine*). See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 14-15. As already indicated earlier, section 11 also contained a restriction upon the disclosure of personal information if there was reason to believe that it would be used for purposes of ADP abroad. Cf. *supra*; nr. 262.
[568] J. Freese, "The Swedish Data Act", *l.c.*, p. 4.

C. Data Inspection Board

273. MISSION – The mission of the Data Inspection Board was to "ensure that ADP does not cause undue encroachment on privacy" (section 15). In addition to its extensive licensing authority (cf. *supra*), the DIB was also charged with monitoring compliance with the Act. Finally, the DIB also served as a department for complaints from the general public.[569]

274. POWERS – Section 16 of the Data Act provided the DIB with the power to inspect any premise where ADP was being carried out or where computers or other equipment was being kept. The same provision also entitled the DIB to access to any documents relating to ADP.[570] The DIB was free to perform such inspections either at its own initiative or pursuant to a complaint.[571] The DIB also had the authority, if it considered it necessary, to alter the regulations it had previously issued, issue new regulations, or revoke a license altogether (section 18). Finally, the DIB also had the authority to issue fines for certain violations of the Data Act (section 24).[572]

2.4 ALLOCATION OF RESPONSIBILITY AND RISK

275. "RESPONSIBLE KEEPER" – The Swedish Data Act allocated the responsibility for compliance with its provisions to the "responsible keeper of a register" ("*registeransvarig*").[573] As the meaning of this term is of central importance to the research objectives of this thesis, several different translations will be considered over the following paragraphs.

276. TRANSLATION BY COUNCIL OF EUROPE – The translation made by the Council of Europe in 1973, reproduced by U. Dammann, O. Mallmann and S. Simitis in 1977, defines the "responsible keeper of a register" as

> "*anyone for whose activity ADP is being carried out, if the register is at his disposal*".[574]

---

[569] C.G. Källner, "Personal Data: The Open Access Approach", *l.c.*, p. 63.
[570] See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 166. Section 17 of the Data Act obliged the responsible keeper of register to deliver to the DIB any "*information and particulars concerning the ADP which the Board requires for its supervision*". This disclosure obligation also applied to anyone who handled a personal register on behalf of the responsible keeper of the register (section 17 *in fine*). See also *infra*; nr. 283.
[571] See also R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 309.
[572] See also *infra*; nr. 286.
[573] See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 167.
[574] U. Dammann, O. Mallmann and S. Simitis (eds.), *Data Protection Legislation. An International Documentation. English – German*, *o.c.*, p. 130.

277. TRANSLATION BY OECD – In 1974, the OECD organized a seminar on the topic of data protection and privacy, the proceedings of which were published in 1976. These proceedings include a translation of the Swedish Data Act in its annexes, where the term "person responsible for a register" is defined as

> "*any person on whose behalf a personal register is kept, if the register is at his entire disposal*".[575]

278. TRANSLATION BY P.G. VINGE – In 1973, P.G. Vinge published one of the earliest commentaries on the Swedish Data Act.[576] In this booklet, the term "responsible keeper" is defined as

> *"the party for whose purposes as personal file is maintained, and who controls the file*".[577]

279. GENERAL CRITERIA – Although there exist notable differences among the translations reproduced here, it seems reasonable to conclude that the concept of a "responsible keeper" consisted of two main components. The first component signals that the responsible keeper was in a sense the "*main beneficiary*" of the personal register: the data processing was carried out "for its activity", "on its behalf" or "for its purposes". The second part of the definition suggests that *mastery* over the register was also an important element: the responsible keeper was an entity who had the register "at his disposal", "at his entire disposal" or under his "control".

280. FROM "FILE KEEPER" TO "RESPONSIBLE KEEPER" – In the early stages of the preparation of the Swedish Act, the term "file keeper" had been used in lieu of the term "responsible keeper".[578] The replacement was reportedly made because the term "responsible keeper" made it clearer that the term referred to the party that actually controlled the file and made decisions on its contents.[579] The concept therefore excluded service bureaus and other parties that might have been involved in the processing of a personal register without actually "controlling" it.[580]

281. "CONTROL" VS. "OWNERSHIP" – As regards the relationship between "control" and ownership, Hondius made a distinction between two scenarios.[581] In the first scenario, the person, enterprise or agency who controls the register is also the owner of the data bank that is used to keep the register. This entity is then considered both the

---

[575] OECD, *Policy issues in data protection and privacy, o.c.*, p. 298
[576] P.G. Vinge, *Swedish Data Act*, *o.c.*, 22 p.
[577] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9. The term "file" refers to the term "personal file", which is Vinge's translation of what we have previously referred to as a "personal register".
[578] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9. As highlighted in the previous footnote, the term "file" refers to the term "personal file", which is Vinge's translation of what we have previously referred to as a "personal register".
[579] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9.
[580] *Id.*
[581] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 101-102.

owner and responsible keeper of the register contained in the data bank. In the second scenario, the data bank used for keeping the register is owned by a party who processes this information for another party (i.e. on its behalf). According to Hondius, it was the decision of the OSK "*to concentrate responsibility with the party that controls the file and orders the data processing operations concerned, and not the party that actually carries out the instructions, such as a service bureau*".[582] This decision was purportedly based on pragmatic considerations, given the widespread practice whereby one data bank would house several different registers.[583] At the time, only very large organisations owned their own data banks, "*and even there a clear distinction [was] drawn between the party that controls the system and the party that operate[d] it under the controller's instructions*".[584]

282. NATURAL OR LEGAL PERSONS – According to P.G. Vinge, both individuals and organisations could be identified as responsible keepers.[585] It seems reasonable to infer that the notion of a "responsible keeper" thus comprised both natural and legal persons, provided the criteria contained in section 1, fourth indent were met.

283. ENTITIES ACTING "ON BEHALF OF" A RESPONSIBLE KEEPER – The Swedish Data Act contained two provisions which explicitly mentioned persons or organisations acting "on behalf of" a responsible keeper. Specifically, section 17 *in fine*, stipulated that the duty to provide the DIB with information was also incumbent upon anyone who handled a personal register on behalf of the responsible keeper.[586] Failure to do so could result in a fine (section 24). In addition, section 13, first indent, included a reference to "any other person who has concerned himself with [a personal register]". This provision, which provided for a general duty of confidentiality (cf. *supra*), also concerned the employees of the responsible keeper as well as service bureaus who acted on its behalf.[587]

284. CIVIL LIABILITY – If a registered individual suffered damage because a personal register contained incorrect information about him, he or she could demand compensation from the responsible keeper of the register (section 23). This provision encompassed a strict tort liability (i.e. no demonstration of fault required), which extended to both economic and non-economic loss.[588]

---

[582] *Ibid*, p. 102
[583] *Id.*
[584] *Id.*
[585] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9.
[586] See also P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 16. Although not spelt out specifically as such in section 16, the DIB's right of access also extended to the premises of third parties such as service bureaus (see section 24). See also J. Freese, "The Swedish Data Act", *l.c.*, p. 5 ("*If the responsible keeper does not have the hardware at its own disposal but resorts to someone else, e.g. a service bureau, the obligations to assist the Board for control purposes will rest on the latter correspondingly*").
[587] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 15.
[588] J. Freese, "The Swedish Data Act", *l.c.*, p. 5. The Data Act did not explicitly provide for civil liability for reasons other than harm suffered from incorrect data processing. However, it seems reasonable to assume that any harm resulting from a failure to observe any of the other duties of a responsible keeper would

285. PUNITIVE PROVISIONS – Section 20 of the Data Act made it a criminal offence for any person to, either wilfully or by negligence, (1) start or keep a personal register without the necessary permission; (2) disregard one of the regulations issued by the DIB; (3) engage in the unauthorized dissemination of personal information; or to (4) provide incorrect information regarding the register to either the DIB or a registered person. The Data Act also created a new category of criminal offence, known as "data trespass", which was defined as unauthorized access or alteration of "recordings for ADP" (section 21).[589]

286. FORFEITURE AND FINES – Section 21 provided that personal registers created or maintained without the necessary permission would be forfeit (unless this would be manifestly unreasonable).[590] Section 24 stipulated that the responsible keeper of a registers, or a person who administers a personal register on his behalf, could be fined if they failed to provide access to the premises or to provide relevant documentation when so requested by the DIB. A responsible keeper could also receive a fine from the DIB for failure to observe the duties of a responsible keeper specified in sections 8, 9 or 10 (section 24 *in fine*).

2.5 CONCLUSION

287. EXPERIMENTAL NATURE – Several commentators have described the Swedish Data Act as an "experiment" or as "a strategy for gaining experience".[591] At the time, the Data Act was seen as part of a gradual development towards regulation of all privacy problems.[592] Like the Hessian Act before it, the Swedish Data Act placed considerable emphasis on the institutional body that would be charged with ensuring compliance.[593] By doing so, the Swedish government hoped to maintain flexibility whilst gaining experience for later policy decisions in this area.[594]

288. A SOURCE OF INSPIRATION – The Swedish Data Act would (also) serve as a source of inspiration for decades to come.[595] In many of its provisions, one can detect precursors to several modern day data protection principles and obligations. Examples include: restrictions regarding sensitive data and international transfers, the use of prior

---

still give rise to remedy under general tort law (albeit that a demonstration of fault would most likely still have been necessary).

[589] See also J. Freese, "The Swedish Data Act", *l.c.*, p. 5.

[590] *Id.*

[591] J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 150. See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 61.

[592] P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 19.

[593] Compare *supra*; nr. 246.

[594] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 169. See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 151.

[595] See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 61.

authorization schemes as a regulatory tool, the duty to ensure accuracy and completeness of information and the granting of rights to data subjects.

289. ALLOCATION OF RESPONSIBILITY – The Swedish Data Act imposed its obligations almost exclusively upon the "responsible keeper of a register". Contrary to the Hessian Act, the Swedish Data Act did provide general criteria to determine which actor was responsible for compliance. These criteria were designed to allocate responsibility with the party that actually "controlled" the register, as opposed to those who were merely passively following instructions. In doing so, the Data Act implicitly exempted, for the most part, service bureaus and other parties that might have been involved in the processing of a personal register but did not actually "control" it.[596] This situation did not, however, detract from the DIB's supervisory authority: even in case of outsourcing, the DIB would be able to effectuate on-site inspection at the premises of a service bureau and it would be obliged to co-operate.[597] None of the provisions of the Swedish Data Act, however, explicitly regulated the relationship between responsible keepers and service bureaux.

290. ALLOCATION OF RISK – The Swedish Data Act allocated the risk of non-compliance primarily with the responsible keeper of the register. Its risk exposure explicitly included (1) liability for damages resulting from the use of inaccurate information (section 23), as well (2) fines levied for failure to abide by the duties of a responsible keeper (section 24). In addition, the Data Act also contained punitive provisions of a more general nature, whose scope was not limited to any specific type of actor (but rather extended to all persons who might interact with the personal information contained in a register).

291. AFTERMATH – Besides being the first country to adopt a national data protection law, Sweden was also the first country to modify a data protection law.[598] It did so in 1979 and 1982, where it introduced changes primarily aimed at limiting registration and licensing requirements.[599] Minor modifications were introduced in 1988 and throughout the early 1990's.[600] Major amendments took again place in 1998, whose principal object was to bring the Data Act in compliance with EU Data Protection Directive 95/46/EC.[601]

---

[596] As indicated earlier, the 1973 Data Act only explicitly addressed persons who handled a personal register "on behalf of" its responsible keeper in two instances, namely in section 17 and section 24 (cf. supra; nr. 283).

[597] Cf. *supra*; nr. 274 and 283.

[598] H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 48.

[599] *Id.* See also R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 307-308; D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 95 and M. Börjesson, "The Swedish Data Act in Transition", in P. Blume (ed.), *Nordic Studies in Information Technology and Law*, Computer/Law Series, Kluwer, 1991, p. 151-162.

[600] See http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Datalag-1973289_sfs-1973-289/ for a complete representation of the amendments to the Swedish Data Act.

[601] For more information on the changes to the Swedish Data Act of 1973 see R. Wong, "The Shape of Things to Come: Swedish Developments on the Protection of Privacy", *SCRIPT-ed* 2005, Vol. 2, Issue 1, p.

3 THE FRENCH LAW ON INFORMATICS, FILES AND LIBERTIES (1978)

3.1 ORIGIN AND DEVELOPMENT

292. COMPUTERS IN THE PUBLIC SECTOR – Similarly to the debates that took place in Hesse and Sweden, the French debate on the use of automated data processing was occasioned by plans to expand computer usage within the public sector.[602] In 1970, the French government proposed two bills which implied increased data sharing among public administrations.[603] The parliamentary debate surrounding these proposals evidenced a need for the elaboration of data protection principles.[604] Although a provision recognizing a general right to privacy was introduced in the Civil Code during that same year[605], the precise meaning of this provision was left largely undefined.[606]

293. LA CHASSE AUX FRANÇAIS – The public debate regarding computers culminated in 1974 as a result of the "Safari" plan, in which it was proposed that all automated files in the public sector should be made accessible by means of one unique identifier.[607] The French newspaper *Le Monde* reported on this plan with an article entitled '*"Safari" ou la chasse aux Français*' ('*"Safari", or the hunt on the French*').[608] This article evoked visions of powerful computers capable of integrating citizen data from all areas of

98-113, available at http://www2.law.ed.ac.uk/ahrc/script-ed/vol2-1/wong.pdf (last accessed 12 August 2013).

[602] F.W. Hondius, *Emerging Data Protection in Europe*, *o.c.*, p. 32.

[603] *Ibid*, 32. The first bill aimed to reinforce traffic safety by integrating information held by the Ministry of the Interior on driver's licenses and that of the Ministry of Justice on convictions for traffic offences (Law n° 70-539 of 24 June 1970 on the centralization of the documentation relative to road traffic), whereas the second bill (i.e. Law of 31 December 1970 on hospital reform) contained a provision aiming to establish a centralized system for electronic health records. (*Id.*) See also R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 256.

[604] F.W. Hondius, *Emerging Data Protection in Europe*, *o.c.*, p. 33-34.

[605] See article 22 of the Law n° 70-643 of 17 July 1970 aimed at strengthening the protection of the rights of individuals and citizens ["*Loi n° 70-643 du 17 juillet 1970 tendent à renforcer la garantie des droits individuels et citoyens*"], Official Journal of the French Republic 19 July 1970, p. 6755, available at http://www.legifrance.gouv.fr.

[606] F.W. Hondius, *Emerging Data Protection in Europe*, *o.c.*, p. 34.

[607] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC. A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector*, Kluwer, Deventer, Computer/Law Series n° 6, 1990, p. 77. ("SAFARI" stood for "Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus") See also R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 256 and D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 166. The report made by the Commission on Informatics and Liberties points out that it was not only the Safari plan, but also the creation of vast data banks and computer networks more generally which gave rise to public concerns. See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, La Documentation Française, Paris, 1975, p. 7. See also H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 49-50.

[608] Ph. Boucher, "« Safari » ou la chasse aux Français", Le Monde, 21 March 1974, p. 9. See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 77.

government.[609] The push towards centralization of governmental files was characterized as a serious threat to individual freedom and the balance of powers.[610]

294. COMMISSION INFORMATIQUE ET LIBERTÉS – The public unrest over the Safari plan further fuelled the call for action, which eventually led to the appointment of a Commission on Informatics and Liberties ("*Commission Informatique et Libertés*" – "CIL").[611] The mandate of this Commission was to propose "measures to ensure that the development of data processing in the public, semi-public and private sectors will take place in the context of respect for private life, individual liberties and public liberties".[612] The CIL concluded that, although the use of informatics had not yet resulted in many infringements of individual liberties, significant risks existed for the future.[613] An increase of social control, together with an aggravation of already unequal relationships within society, were perceived as key areas of concern.[614]

295. LEGISLATIVE DEVELOPMENT – The CIL report, which was published in 1975, was accompanied by a preliminary draft bill aimed at regulating the processing of personal information.[615] This draft bill served as the basis for the subsequent proposal put forth by the French government in 1976.[616] After substantial modifications by the Senate, the bill was accepted by both houses of Parliament in December of 1977.[617] It was enacted on 6 January of 1978 as Law n° 78-17 concerning Informatics, Files and Liberties (LIFL).[618]

---

609 Ph. Boucher, "« Safari » ou la chasse aux Français", *l.c.*, p. 9.

610 *Id.*

611 Decree n° 74-938 of 8 November 1974 establishing the Committee on Informatics and Liberties ["*Décret n°74-938 du 8 novembre 1974 portant création de la Commission Informatique et Libertés*"], Official Journal of the French Republic 13 November 1974, p. 11403, available at http://www.legifrance.gouv.fr. See also Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, La Documentation Française, Paris, 1980, p. 8.

612 Article 1 of Decree n° 74-938. See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 166. The CIL did not need to start its work from scratch. In addition to the studies carried out in other countries, the CIL could also benefit from studies carried out by the French Conseil d'Etat et Chancellerie carried out in in 1971 and 1972 respectively. (Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 7)

613 Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 11-17.

614 *Ibid*, p. 17. See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 166.

615 While the report of the CIL was made public, the draft bill itself was not. (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 78.)

616 Assemblé Nationale, *Projet de loi relatif à l'informatique et aux libertés*, Enregistré à la Présidence de l'Assemblée national le 9 aout 1976, Annexe au procès-verbal de la séance du 2 octobre 1976, Document Parl. no. 2516, p. 1-18, available at http://www.senat.fr/leg/pjl76-2516.pdf (See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 78.)

617 See Commission nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 9 ; R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 257 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 78.

618 Law n° 78-17 of 6 January 1978 concerning informatics, files and liberties ["*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*"], Official Journal of the French Republic 7 January 1978, p. 227-231. (corr. 25 January 1978), available at http://www.legifrance.gouv.fr. The legislative development of this law can be tracked at http://www.senat.fr/dossier-legislatif/pjl77-005.html.

3.2 SCOPE

296. PUBLIC AND PRIVATE SECTOR – The LIFL applied to both public and private sector data processing (art. 14).[619] However, as will be made clear over the following paragraphs, a different regime applied to public and private data processing respectively.

297. AUTOMATED, NON-AUTOMATED AND MECHANIZED PROCESSING – The LIFL governed automated, non-automated and mechanized processing of personal data.[620] Article 5 defines automated processing as

> "*any set of operations, performed by automatic means, relating to the collection, recording, development, modification, storage and deletion of personal data as well as any set of operations of a similar nature relating to the use of files or data bases, in particular the interconnection or linkage, consultation or communication of personal data*".[621]

The notions of "non-automated" and "mechanized" (or "machine") processing of personal data were not further defined in the law.[622] Although most of the law affected only the automated processing of personal data, several of its provisions also applied to non-automated or mechanized files.[623]

298. PERSONAL DATA – The LIFL applied to the processing of personal data ("*informations nominatives*"), which are defined by article 4 as "*data which permit, in any form, directly or indirectly, the identification of natural persons to whom they relate*".[624]

---

[619] See also J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 157 (noting that while article 14 essentially served to articulate the duties of the CNIL, it also identifies the scope of the LIFL.

[620] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 81.

[621] The translations of the provisions of the LIFL in this section are based on the original version of the LIFL, together with the translation provided by A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 81 et seq. Generally speaking, the concept of "processing" was intended to refer to processing *systems* (i.e. sets of processing operations) rather than individual data processing operations (see Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 25). However, certain provisions did also refer to specific data processing operations such as the collection, storage or access to data.

[622] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 81-82.

[623] D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 175. See article 45 LIFL (specifying that articles 25, 27, 29-33 also applied to the non-automated and/or mechanized processing of personal data unless such processing was intended exclusively for personal use ("*dont l'usage relève strict exercice du droit à la vie privée*") (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 82.). The argument for including non-automated and mechanized processing within the scope of the LIFL was to avoid 'privileging' non-automated techniques over automated ones, as well as to avoid circumvention of the law (Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 21). See also N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *La Revue adminstrative* 1983, Vol. 36, no. 215, p. 453, available at http://www.jstor.org/stable/40775313?seq=1 and P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, Economica, Paris, 1984, p. 289-290 (highlighting that the inclusion of non-automated files in the scope of the LIFL was also driven by the risks they presented).

[624] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 82. The LIFL thus did not apply to the processing of data concerning legal persons, although this had been the intention of the initial

299. EXEMPTIONS AND DEROGATIONS – The LIFL provided for certain exemptions to its scope, as well as derogations to a number of its provisions. For example, non-automated or mechanized of personal data was exempted entirely from the law if such processing was intended purely for personal use (e.g., addresses entered into a personal diary).[625] A partial derogation was also provided for processing of personal data by entities of the press.[626] In addition, article 17 also created the opportunity for the issuance of "simplified rules" for processing that did not present a danger to individual privacy or basic freedoms (cf. *infra*; nr. 304).[627]

3.3 BASIC PROTECTIONS

300. OVERVIEW – The LIFL sought to protect privacy and individual liberties by (1) putting in place procedures for prior consultation or declaration; (2) imposing a number of restrictions and obligations in relation to the processing of personal data; (3) providing individuals whose data were being processed with certain rights and (4) establishing a National Committee on Informatics and Liberties (CNIL) endowed with broad supervisory powers.

A. Prior consultation or declaration

301. PUBLIC SECTOR – Pursuant to article 15, automated processing of personal data on behalf of a public or semi-public[628] entity required a legal or regulatory basis.[629] This law or regulation could only be adopted after obtaining a motivated opinion from the

---

government draft bill. See A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *La Revue Administrative* 1978, Vol. 31, n° 181, p. 32 and P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 290-291.

[625] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 82 (based on art. 45 LIFL). This exemption was said to encompass "non-professional" files, which are "not related to any activity which places those that hold them in an "organisational" relationship [*rapport organique*] with third parties" (A. Holleaux, "La loi du 6 janvier 1978 sur l'informatique et les libertés (II)", *l.c.*, p. 165). *Automated* processing of personal data by individuals would, strictly speaking, fall within the remit of the LIFL, even if it were carried out for a purely private purpose. See N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *La Revue adminstrative* 1983, Vol. 36, no. 215, p. 465.

[626] See article 33 LIFL.

[627] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 82. It is interesting to note that the LIFL did apply, as a matter of principle, to matters concerning national security, defense and public safety. Several provisions of the LIFL did however contain specific derogations for such instances. See e.g. art. 19 (contents of request for an opinion); art. 39 (right of access).

[628] In addition to "the State", article 15 also mentions "public institutions" ("*établissement public"*), institutions of a collective territory ("*établissement d'une collectivité territoriale*") and private legal persons operating a public service ("*personne moral de droit privé gérant un service public*").

[629] Whether or not a formal law was required (or another form of regulation might suffice) was determined by article 34 of the French Constitution. See A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *l.c.*, p. 35-36 and P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 295-298.

CNIL.[630] In case of an unfavourable opinion, the processing could only take place on the basis of a decree which was adopted in accordance with an opinion issued by the Council of State (article 15, second indent).[631]

302. PRIVATE SECTOR – Processing of personal data on behalf of private sector entities[632] was not subject to a requirement of prior consultation, but rather to a declaration procedure (article 16). Any private sector entity seeking to initiate personal data processing first needed to submit a declaration to the CNIL. Upon submission, the CNIL would verify whether all the requisite information was included in the declaration. If so, it would issue a receipt. Only upon obtaining this receipt would the applicant be allowed to initiate the processing (article 16, second indent).[633]

303. CONTENT OF A REQUEST OR DECLARATION – Article 19 enumerated the different elements that needed to be included in a request for an opinion or declaration.[634] Both types of documents were required to specify[635]:

- the identity of the person presenting the request [or declaration], as well as the identity of the *person who has the power to decide whether personal data shall be processed* ("*celle qui a pouvoir de décider la création du traitement*")[636];
- the *characteristics*, *purposes*, and, if applicable, the *name* of the processing;
- the department or the departments *responsible for implementing the processing*;

---

[630] Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 24. In situations where the processing of personal data required a basis in law, the government was required to attach the opinion of the CNIL to the draft bill when submitting it to Parliament (article 20 of the Decree of 17 July 1978). (N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 453)

[631] Due to the requirement of a favorable opinion by CNIL or Council of State, one might argue that the requirement prior consultation was in fact a system of prior authorization or licensing (similar to the procedure that existed in Sweden). While the withholding of a favorable opinion could have similar effects in practice, it would be more correct to view the French system of prior consultation as a procedure to ensure that privacy considerations are taken into account, rather than as a formal licensing procedure. (see J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 165).

[632] Article 16 mentioned "entities other than those subject article 15".

[633] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 92. The primary objective of the declaration procedure was to ensure that the CNIL remained abreast of technological developments within society, rather than to create a procedure of prior approval (see Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 34). However, the CNIL did have the authority, if it deemed it appropriate, to issue recommendations regarding the declared processing (N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 454). If necessary the CNIL also had the ability to bring matters to the attention of the Prosecutor's office (article 21, 4° LIFL). (see also Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 34.)

[634] Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 24.

[635] Translation based on the original version of the LIFL and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 80 and p. 93.

[636] In case this person resided outside of France, the name of his or her representative in France was to be provided (article 19, first indent).

- the department where the *right of access* provided by chapter 5 can be exercised as well as the measures taken to facilitate the exercise of these rights;
- the *categories of persons who*, by reason of their duties or for the needs of the department, *have direct access to the registered data*;
- the *personal data processed*, their source, the *duration* for which they shall be stored, as well as the *recipients or categories of recipients* authorized to receive these data;
- the *links, interconnections or any other form of linkage* of these data as well as their transfer to third parties;
- the steps taken to ensure the *security of processing and data* and to guarantee secrets protected by law;
- whether the processing is intended for *dispatch of personal data between the French territory and a foreign country*, in any form, including the case where it involves operations carried out partly in France on the basis of operations previously carried out outside of France.

Any modification relating to the information listed above, or any cancellation of processing, was to be notified to the CNIL (article 19). In case of data processing based on a regulatory act, the act in question was required to specify several of the elements listed above (article 20).[637]

304. "SIMPLIFIED RULES" – Article 17 LIFL allowed the CNIL to adopt so-called "simplified rules" ("*normes simplifiées*") for very common types of processing, provided they "*clearly do not pose any risk to privacy or freedom*" ("*qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés*"). Such simplified rules could be adopted vis-à-vis both private and public sector data processing. In situations where "simplified rules" applied, the actor responsible for such processing needed only to declare that the processing conformed to their provisions (rather than submitting a request or declaration of its own) (article 17, second indent).[638]

[637] The regulation in question would have to specify in particular (1) the name and purpose of the processing; (2) the department where the right of access provided by chapter 5 can be exercised, as well as (3) the categories of registered information as well as the recipients or categories of recipients authorized to receive these data.

[638] See also Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 31 et seq. and N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 454. Early examples of such simplified rules concerned processing in the areas of human resource management, utility consumption, loaning of books, tax collection, etc. (Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 33-34.)

B. Data processing requirements

305. OVERVIEW – In addition to the procedures of prior consultation and declaration, the LIFL also articulated a number of restrictions and obligations. In particular, the LIFL contained (1) general principles concerning the use of information technology; (2) rules concerning the collection and storage of personal data; (3) a requirement of security of processing; and (4) restrictions upon the use of sensitive data and national identification numbers.

306. GENERAL PRINCIPLES – Article 1 provided that

> "*Informatics must be at the service of every citizen. […]*
> *It shall infringe neither human identity nor the rights of man, nor private life, nor individual or public liberties*."

The broad language of this provision reaffirmed that the concerns regarding the use of informatics were not limited to the issue of privacy. One of the basic premises of the drafters of the LIFL was that information technology had the ability to affect all areas of community and social life, not merely the private life of individuals.[639]

307. PROFILING – Article 2 provided that "*no judicial decision involving an assessment of human behaviour may be based on an automated processing of data which describes the profile or personality or the individual concerned*". A similar restriction was articulated in relation to administrative and private decisions. However, the impact of this latter provision was limited significantly due to the additional qualification that automated processing may not be "sole" basis of the decision (article 2, second indent).[640]

308. DATA COLLECTION – The drafters of the LIFL sought to "discipline" the collection and recording of personal data in several ways.[641] As indicated earlier, any automated processing of personal data first needed to be included in a request for an opinion or a declaration (cf. *supra*). As part of its supervisory activities, the CNIL would also check whether these data were in fact necessary to realize the stated purpose of the processing.[642] If not, the CNIL would seek to limit any collection it deemed excessive.[643]

---

[639] See A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 79. In its report, the CIL had underlined that informatics had the ability to affect more than just the private life of individuals (even though the latter had admittedly been the focus of its attention). See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 29 et seq. Even though the bulk of the provisions of the LIFL focus on regulating the automated processing of personal data, the broad language of article 1 led the CNIL to construe its mission in an equally broad fashion. See D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 176-177.

[640] For more information regarding the rationale underlying this provision see A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *l.c.*, p. 32.

[641] See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 45-49.

[642] N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 460. Although this requirement of "collection limitation" cannot be found explicitly in the original version of the LIFL, it appears to have been

Finally, article 25 provided that the collection of personal data by fraudulent, dishonest or illegal means was prohibited. For example, it would be unlawful to collect personal data from files which were not intended for third-party disclosure.[644]

309. FINALITY – The principle of finality was a fundamental principle of the LIFL.[645] Each request for an opinion or declaration needed to state the purpose(s) of the processing (cf. *supra*).[646] This stated purpose would then in principle determine the authorized usage of the collected data.[647] Any use of personal data for purposes other than those mentioned in the request for an opinion or declaration was illegal (article 44).

310. ACCURACY AND COMPLETENESS – If the entity holding a file containing personal data obtained knowledge of its inaccuracy or incompleteness, these data were to be corrected or completed (article 37). Should these data have previously been disclosed to a third party, the entity was in principle also obliged to notify them of the correction (article 38).[648]

311. STORAGE LIMITATION – Article 28 provided that "*unless otherwise provided for by law, personal data may not be stored in personal form beyond the period stated in the request for an opinion or declaration, unless such storage is authorized by the commission*". The provision was based on the recommendation made by the CIL that data should not be stored indefinitely, but rather be preserved only as long as they are useful for the purposes of the processing.[649]

---

a matter of administrative practice, inspired by the laws of other countries. See Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 27. The CIL had previously also noted the importance of the rule according to which "only data corresponding to a legitimate purpose should be taken into account". See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 48-49.

[643] N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 460.

[644] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 89.

[645] N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 459. See also Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 53-54.

[646] For each declaration or request for an opinion, the CNIL would verify (1) whether the stated purpose was compatible with the duties ("*missions*") of the declaring entity and (2) whether the recorded data corresponded to the stated purpose. (N. Lenoir, *l.c.*, p. 459.)

[647] The same processing operations could in principle serve multiple purposes. The CNIL also allowed certain "extensions" to the purposes of the processing, in particular for statistical or research purposes. N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 459.

[648] This obligation existed unless the CNIL exempted them from it (art. 38 *in fine*).

[649] Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 50. See also D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 180. See also A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *l.c.*, p. 38-39.

312. SECURITY – Article 29 stipulated that

> *"any person ordering or performing a processing of personal data shall commit himself, towards the individuals concerned, to see that all necessary precautions are taken to protect the and in particular to prevent these from being distorted, damaged or disclosed to unauthorized third parties*".[650]

This obligation to ensure security of processing was also reflected in the punitive provisions of the act (cf. *infra*; 332).[651]

313. SENSITIVE DATA – The LIFL imposed additional restrictions on the processing of certain types of "sensitive" data. These data were regarded as sensitive either because of their intimate nature or because they could readily serve as a basis for unfair discrimination.[652] The restrictions concerned data regarding criminal offences, convictions or security measures (article 30), as well as data revealing racial origin, political, philosophical or religious opinions, or union membership (article 31). Processing of these data was generally prohibited. Data regarding criminal offences, convictions or security measures could in principle only be processed by "*the jurisdictions and public authorities acting within the scope of their legal powers and, on the favourable opinion of the national commission, companies managing public services*".[653] Data revealing racial origin, political, philosophical or religious opinions, or union membership could in principle only be processed with the express consent of the individual concerned.[654]

314. NATIONAL IDENTIFICATION REGISTER – Article 18 stipulated that the use of the national identification register of national persons ("*répertoire national d'identification des personnes physiques*") was to be authorized by a decree from the Council of State, adopted after receiving an opinion from the CNIL. The terms "use of the national register" was interpreted broadly. It referred not only to the consultation of this register, but also to any use of the national register number (e.g., for purposes of identification or interconnection).[655]

---

[650] See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 63 et seq. for a discussion of security measures envisaged by the CIL.

[651] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 95. See also A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *l.c.*, p. 38.

[652] Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 47.

[653] Translation by D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 180.

[654] Exceptions to this rule of express consent were provided for religious, philosophical, political or organisations who kept an automated record of data regarding their members or correspondents (art. 31, second indent). In addition, other exceptions to this rule could be adopted for reasons of public interest, on the Commission's proposal or favourable opinion by a decree made by the Council of State (art. 31, second indent). See also N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 455; D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 180; P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 306-310 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 90.

[655] See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 55 et seq.; Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la*

315. INTERNATIONAL TRANSFERS – Article 24 provided that

> *"the transfer, between the French territory and a foreign country, in any form, of personal data whose automated processing is governed by article 16 [...], can be made subject to a requirement of prior authorization or regulation in accordance with terms established by a decree issued by the Council of State [...]*".

The reason why this article only expressly targeted private sector data processing was because public sector data transfers could protected by means of the legal or regulatory act providing a basis for the processing.[656]

C. Data subject rights

316. OVERVIEW – The LIFL accorded individuals whose personal data was being processed ("*personnes concernées"*) a number of rights, including (1) a right to be informed; (2) a right to object; (3) a right to access; (4) a right to know and to contest; and (5) a right to correction.

317. RIGHT TO INFORMATION – Article 27 provided that individuals, from whom personal data are collected, shall be informed of:

- whether providing the solicited information is mandatory or optional;
- what consequences they might face in case of a failure to respond;
- the natural or legal persons that will be recipients of the information;
- the existence of a right of access and rectification.[657]

318. RIGHT TO OBJECT – Article 26 provided that individuals shall have the right to object to the processing of their personal data. Such an objection would have to be founded on a legitimate reason. Whether or not a legitimate reason existed was not further defined by the LIFL and therefore needed to be decided on a case-by-case basis.[658]

319. RIGHT TO ACCESS – Every individual had a right to obtain, from any actor or service engaged in the processing of personal data, (1) confirmation as to whether or

---

République et au Parlement 1978-1980, *o.c.*, p. 29-30 and N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 455. Because of the close relationship between the national register number ("*Numéro d'Inscription au Repertoire*" – NIR) and the identification number used by the social security administration (the latter being identical to the former with the addition of a three-digit number), both numbers were regulated in the same fashion. (*Id.*)

[656] A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I)", *l.c.*, p. 36. See also P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 348-350.

[657] For more information see A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 85

[658] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 85-86. See also A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés", *l.c.*, p. 37-38.

not data about them was being processed and, if so, (2) to have these data communicated to him (article 34).[659] No motivation was necessary to justify an access request.[660] The individual concerned needed only to prove his or her identity and submit the request in accordance with the modalities stipulated by the CNIL.[661] Obtaining a copy of one's personal data could be subjected to a flat fee established by the CNIL (article 35, second indent).[662]

320. RIGHT TO KNOW AND TO CONTEST – In addition to the right to object and the right of access, the LIFL also provided individuals with a right to contest the processing of their personal data. Specifically, article 3 provided that every person had the right "*to know and contest the information and reasoning used in automated processing of which the results are used against him*". This provision implied that an individual had a right to learn, not only what data about him were being processed, but also what the logic was of the processing itself (at least in situations where the results of this processing were used against him).[663]

321. RIGHT TO CORRECTION, COMPLETION OR CLARIFICATION – Finally, articles 36 also provided individuals with a right to correction. Specifically, article 36 stipulated that "*the holder of a right of access may demand that any data regarding him which are incorrect, incomplete, ambiguous or outdated be corrected, completed, clarified or deleted*". The same right existed in relation to data of which the collection, use or communication was prohibited.[664] If the individual so requested, the department or entity concerned had to send him a copy of the modified data free of charge (article 36, second indent).[665]

---

[659] A discussion of the rationale behind this provision can be found in Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 37-43. It is worth noting that the right of access was perceived as complementary to the public's ability to access the list of processing operations maintained by the CNIL (art. 22 LIFL; cf. *infra*). By consulting this list, it was reasoned, individuals would be capable of determining in which files personal data about them might be included (if they did not know already) and learn where they might obtain more information. See also N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 463.

[660] N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", *l.c.*, p. 463.

[661] *Id*. Where medical data were concerned, however, the right of access was to be exercised via a doctor (article 40 LIFL). Where the processing activity affects national security, defense, or public safety, the right of access was to be exercised via the CNIL (article 39). See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 85-86.

[662] For more information regarding the right of access see A. Holleaux, "La loi du 6 Janvier 1978 sur l'informatique et les libertés (II)", *l.c.*, p., 160-163.

[663] See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 84-85.

[664] In cases of data processing concerning national security, defense and public safety, to right to correction was to be exercised via the CNIL (article 39).

[665] In case of a modification, the individual concerned was also to be reimbursed for any charges levied pursuant to the exercise of the right of access (article 36, third indent). As indicated earlier, the entity holding the file was in principle also obliged to notify any third parties to whom this information had previously been disclosed (article 38) (cf. *supra*).

D. National Committee on Informatics and Liberties (CNIL)

322. MISSION – The National Committee on Informatics and Liberties ("*Commission Nationale Informatique et Liberté*" – "CNIL") was established to

> *"ensure compliance with the provisions of [the LIFL], in particular by informing all individuals concerned of their rights and obligations, by consulting with them and by supervising the use of informatics for the processing of personal data*".[666]

The mission of the CNIL was thus to inform, advise and supervise individuals engaged in (or affected by) the processing of personal data.[667] In addition, the CNIL was also responsible for maintaining a publicly available list of all public and private data processing (article 22 LIFL). This list was to specify, for each processing system:

- the law or regulatory act which decided about the creation of the processing or the date of its declaration;
- its name and its purpose;
- the service with which one can exercise one's right of access;
- the types of personal data registered as well as the recipients or categories of authorized recipients.

323. POWERS – The LIFL endowed the CNIL with broad supervisory powers. In addition to its authority to review declarations or requests for private and public sector data processing, as well as to issue simplified norms (cf. *supra*), the CNIL also had the authority to (article 21):

- conduct investigations and on-site inspections;
- develop recommendations and model regulations regarding the security of processing;
- receive and mediate complaints;
- render certain decisions in specific cases (e.g., to allow an exception to the granting of a right of access[668]);
- issue warnings and inform the public prosecutor of any infractions that come to its knowledge; and
- propose any legislative or regulatory measure it deemed appropriate to protect individual freedoms in light of technological developments.[669]

---

[666] Article 6 LIFL.

[667] The exercise of these tasks could take on a variety of forms. See Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 71; Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 16-17 and A.C.M., *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 96-97.

[668] See article 35, second indent LIFL.

The entities in charge of (public or private) organisations, as well as the entities that hold or use files containing personal data were obliged to co-operate with the CNIL in the exercise of its tasks (art. 21 *in fine*).

3.4 ALLOCATION OF RESPONSIBILITY AND RISK

324. ABSENCE OF A FORMAL DEFINITION – The 1978 LIFL did not formally define which actor (or type of actor) would be responsible for compliance with its provisions. Instead, the LIFL articulated its commands either in general terms (as generally applicable requirements or prohibitions) or by imposing certain responsibilities on specific entities (using varying terminology).

325. CIL REPORT: PUBLIC SECTOR – The CIL report, which had preceded the drafting of the LIFL, stated that the responsibilities of each actor involved in the processing of personal data should be clearly specified.[670] In case of public sector data processing, the CIL expected that the law or regulation, which was to provide the legal basis for the processing, would also specify the responsibilities of the different entities involved.[671] In this regard, it considered it insufficient that the act in question

> "*would limit itself to the declaration that a minister or manager was the 'master' of a particular file. While it is good to affirm the responsibility for the whole (with regard to its finality, its general organisation and its supervision), one must also decompose the processing in its successive operation, without ignoring that which precedes it, accompanies it, or follows it, and decide who must do what*"[672]

As far as the local communities and public institutions were concerned, the CIL considered it equally necessary for them to define and distribute responsibilities amongst each other.[673] In regard to the allocation of risk, the CIL noted that

> "*[i]f the processing of personal data were to cause harm to a third party, the community would be liable. However, it is not sufficient for the mayor or secretary general to push himself forward to cover their subordinates. The mission and duties of each must be specified and it must be possible to identify the people who were really responsible*."[674]

---

[669] See also Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 16-17; D.H. Flaherty, *Protecting Privacy in Surveillance Societies*, *o.c.*, p. 186-188 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 97-101.

[670] Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 69.

[671] *Id.* See also p. 31-32 of the same report.

[672] *Id.* For example, the head of one particular administrative agency might be responsible for certain operations and for part of the security of the processing, but not be responsible for the collection of the data or what happens to the data once it's been transmitted to its intended recipients. Also, in the event a security officer is appointed, this person would have certain responsibilities without "absorbing" the responsibilities of others. (*Id.*)

[673] *Id.*

[674] *Id.*

326. CIL REPORT: PRIVATE SECTOR – The CIL report was extremely succinct with regards to the allocation of responsibility for private sector data processing. It merely stated: "*similar considerations seem to be valid*".[675] As regards allocation of risk, the CIL noted that

> "*it hopes that the use of informatics will not present an occasion to excessively multiply [the number of] criminal offences, nor to create instances of vicarious criminal responsibility. [The Commission] also considered that the general principles of civil liability should be sufficient, at least for a while, to ensure compensation for damages suffered*".[676]

327. INCONSISTENT TERMINOLOGY – Both the CIL report and the LIFL used various terms to identify the actor (or actors) responsible for ensuring compliance. For example, the CIL report at times spoke of "the entity responsible for the file" ("*l'organisme responsable du fichier*") and the holder of the file ("*détenteur du fichier*").[677] The LIFL itself employed an even wider variety of terms, which included:

- entities "on whose behalf" ("*pour le compte de*") data processing is taking place (articles 15-16)[678];
- the "person who has the power to decide whether personal data shall be processed" ("*celle qui a pouvoir de décider la création du traitement*") (article 19)[679];
- the department or departments charged with implementing the processing ("*le service ou les services chargés de mettre en œuvre le traitement*") (article 19)[680];
- the "holders" or "users" ("*les détenteurs ou utilisateurs*") of the files (article 21)[681];
- a "person ordering or performing" ("*toute personne ordonnant ou effectuant*") the processing of personal data (article 29)[682];
- "entities charged with performing the processing" ("*organismes chargées de mettre en œuvre le traitement*") (article 34)[683];
- the entity responsible for the file ("*le responsable du fichier*") (article 35)[684]

---

[675] *Ibid*, p. 70.
[676] *Id.*
[677] See e.g. Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 42-44. In relation to private sector data processing, the CIL also referred to "private actors that manage personal files or have them managed by third parties" (as responsible entities who must submit a declaration). (*Ibid*, p. 34).
[678] Articles 15 and 16 concerned the obligation to submit a request for an opinion or declaration. Cf. *supra*; nrs. 301 et seq.
[679] Article 19 concerned the contents of a request or declaration. Cf. *supra*; nr. 303.
[680] Id.
[681] Article 21 concerned the obligation to co-operate with members to the CNIL in the exercise of their tasks. Cf. *supra*; nr. 323.
[682] Article 29 concerned the obligation to ensure the security of processing. Cf. *supra*; nr. 312.
[683] Article 34 concerned the right of access of individuals. Cf. *supra*; nr. 319.
[684] Article 35 also concerned the right of access of individuals. Cf. *supra*; nr. 319.

- the entity holding the file ("*l'organisme qui le tient*") (article 37).[685]

328. GENERAL CRITERIA – Although the LIFL did not formally define its scope *ratione personae*, it did contain criteria that could be used to identify "the responsible entity". Basing itself on article 19, the CNIL concluded that the entity that should submit a declaration ("*organisme déclarant*") was "the physical or legal person who has *the power to decide* about whether personal data shall be processed".[686] The language of articles 15-16 suggested that this "*organisme déclarant*" was also the entity "*on whose behalf*" ("*pour le compte de*") personal data processing would be taking place.[687] As a result, it seems reasonable to conclude that the (implicit) concept of a "responsible entity" under the LIFL was akin to that of a "responsible keeper" under the Swedish Data Act: both the element of *mastery* (decision-making power) and of *benefit* ("on its behalf" were incorporated in the law's provisions.[688]

329. ENTITIES ACTING "ON BEHALF OF" – The LIFL also contained several provisions referring to persons or organisations that might be processing personal data on behalf of others. For example, articles 19, 29 and 34 referred to entities "performing the processing".[689] Articles 21 and 37 likewise referred to the "holders" of the file. These provisions made clear that entities who performing data processing on behalf of others also faced certain responsibilities and restrictions.[690] For example, any "holder" of a file containing personal data was obliged to co-operate with the members to the CNIL in the exercise of their tasks (article 21). He or she was seemingly also obliged to rectify or complete inaccurate or incomplete information upon obtaining knowledge of its incompleteness or inaccuracy (article 37).[691] Data subjects also had the ability to

---

[685] Article 37 concerned the right of correction. Cf. *supra*; nr. 321.

[686] Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 26. By way of example, the CNIL noted that an entity who both initiates and performs the processing of personal data would meet this concept. The same qualification would apply, however, to an entity that initiates the processing but outsources its operations to a third party. In situations whereby one entity initiates the processing of personal data, then transfers some of these data to a third party, who then processes them further for his own account, both these entities would be considered responsible for submitting a declaration. (*Id.*)

[687] This interpretation is also implicitly confirmed by the examples provided in the first activity report of the CNIL (Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 26).

[688] Compare *supra*; nr. 327. The decision-making power of "responsible entities" under the LIFL in principle concerned every aspect of the processing (its organisation, collection methods used, etc.). First and foremost, however, it concerned the decision to *initiate* the processing of personal data ("*décider la création*"). See also Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 29-31 (which referred to "*la décision de recourir à l'informatique*" and "*la décision d'entreprendre traitements*").

[689] According to the CNIL, the reference in article 19 to "the department or departments charged with implementing the processing" ("*le service ou les services chargés de mettre en œuvre le traitement*") referred to the entity or entities who were appointed by the "*organisme déclarant*" to act as its "technical contact point(s)" ("*interlocuteur technique*"). See Commission Nationale de l'Informatique et des libertés, *Premier rapport au Président de la République et au Parlement 1978-1980*, *o.c.*, p. 26.

[690] *Contra*: A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 96.

[691] Article 37 makes a reference to "l'organisme qui le tient". Given the earlier reference to "*détenteurs ou utilisateurs*" (article 21), it seems reasonable to infer that article 37, by using the verb "to hold" ("*tenir*") in

exercise their right of access vis-à-vis the entities charged with performing the processing (article 34). Finally, the obligation to ensure security of processing, was also incumbent on those who performed the processing of personal data (article 29).

330. A SHARED RESPONSIBILITY – Based on the foregoing considerations, one can conclude that the responsibility for ensuring compliance with the LIFL was shared, at least in part, among (1) those who had made the decision that personal data processing should take place (*la personne "ordannant" ou* "*décidant la création*") and (2) those engaged the actual performance to the processing (*ceux qui "mettent en oeuvre" ou "performent"*). In certain provisions, the allocation of responsibility upon either (or both) types of actor was explicit. In other provisions such explicit allocation was absent, meaning that the precise nature and scope of each actor's obligations would have to be analysed on a case-by-case basis.

331. DEGREE OF FLEXIBILITY - While certain provisions of the LIFL specified which actor (or actors) should comply with its prescriptions, there were many requirements for which the "responsible entity" was free to determine how compliance would be ensured - and by whom.[692] As indicated earlier, the CIL report had called for a clear specification of the responsibilities among actors involved in the processing of personal data.[693] Particularly in the case of outsourcing, the CIL wished to draw attention to the

> "*risk that, if strict precautions are not taken with regard to the mission delegated in a service contract, and then in an outsourcing contract, it would become difficult to know what the responsibilities of each entity are*".[694]

In order to address this risk, the CIL suggested that the supervisory authority charged with overseeing the law (i.e. the CNIL) would develop or approve standardised agreements for these situations.[695]

---

first instance referred to the entity who actually "held" the file (which would not necessarily be the same as the entity who "ordered" the processing to take place). However, given that the absence of a formal terminology, one must be cautious in concluding that this provision applied only to a certain type of entity (the holder or "*détenteur*") and not the other (the "responsible entity" or "*organisme declarant*"). In any event, it seems reasonable conclude that the individual concerned had the ability to request the correction or completion of information directly from the entity holding his or her data, without having to first contact the "*organisme déclarant*" (in situations where the "holder" and "declarer" or the processing were not the same entity).

[692] Undertaking this exercise was (at least in part) necessitated by article 19, which mandated the inclusion of certain elements in any request for an opinion or declaration (e.g., a designation the department or departments "implementing" the processing; a designation of the department or departments where the right of access can be exercised; indication of steps undertaken to ensure the security of processing). Cf. *supra*; nr. 303.

[693] Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 69. Cf. *supra*; nr. 325.

[694] *Ibid*, p. 70.

[695] *Id.* Strictly speaking this remark only concerned processing operations undertaken on behalf of public sector entities. However, the following sentence in the CIL's report is that "*similar considerations seem to apply for the private sector*". The CIL also noted that "*the contracts usually offered to users by manufacturers or service providers are quite inconspicuous about the obligations of service providers and it would opportune to seek out more balanced formulations*" (*Id.*).

332. PUNITIVE PROVISIONS – The LIFL provided for a number of new criminal offences in articles 41-44 of the law. Article 41 made it a crime for anyone "to carry out or have others carry out" ("*aura procédé ou fait procéder*") automated processing of personal data before (a) publication of regulatory act authorizing the processing or (b) having submitted the requisite declaration.[696] Article 42 criminalized the registration or storage of data in violation of articles 25 (collection of personal data by fraudulent, dishonest or illegal means), 26 (legitimate objection by data subject), 28 (limitation of storage duration), 29 (security of processing), 30 and 31 (sensitive data).[697] Article 43 made it a crime for anyone to engage in an unauthorized disclosure of personal data that would damage the reputation of the person concerned, as well as the intimacy of his or her private life.[698] Finally, article 44 penalized any entity that used personal data for a purpose other than the one defined in the declaration or regulatory act authorizing the processing.[699]

333. CIVIL REMEDY – The LIFL did not contain any specific provisions concerning damages resulting from a violation of the law.[700] Normal rules regarding civil liability would apply in those cases.[701]

[696] Violation of this provision was punishable by a fine and/or imprisonment of not less than 6 months with a maximum of 3 years. In addition, a convicted person could also be ordered by the courts to publish the sentence (in part or in full) at his own expense (article 41, second indent). (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 102.) See also P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 292.

[697] Violation of this provision was punishable by a fine and/or imprisonment of not less than 1 year with a maximum of 5 years. Again, the convicted person could also be ordered by the courts to publish the sentence (in part or in full) at his own expense (article 42, second indent). (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 102-103.)

[698] Violation of this provision was punishable by a fine and/or imprisonment of not less than 2 months with a maximum of 6 months. (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 103.)

[699] Violation of this provision was punishable by a fine and/or imprisonment of not less than 1 year with a maximum of 5 years. (A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 103.)

[700] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 105.

[701] *Id.* See also supra; nr. 326 (noting that the CIL had considered that the general principles of civil liability should be sufficient, at least for a while, to ensure compensation for damages suffered). (Commission Informatique et Libertés, *Rapport de la Commission Informatique et libertés*, *o.c.*, p. 70.)

3.5 CONCLUSION

334. STAYING THE COURSE – The French Law on Liberties, Informatics, Files and Liberties followed the footsteps of its German and Swedish predecessors. In some respects it bore resemblance to the data protection laws of Hesse[702] and the Federal Republic of Germany[703], in others it more closely resembled the Swedish Data Act[704]. Many of its key provisions, such as the right of access, the limitation of storage duration and the right to know still echo in contemporary data protection legislation.

335. ALLOCATION OF RESPONSIBILITY AND RISK – The LIFL did not formally define which actor (or type of actors) would be responsible for compliance with its provisions. Instead, it employed a range of different terms to refer, on the one hand, to the actor that carried primary responsibility for the processing (i.e. the entity that "decided about the creation of data processing", "ordered" the processing or "carried out or had others carry out" personal data processing) and, on the other hand, to actors who might be engaged in the processing of personal data on behalf of others (i.e. the entities "performing the processing", the "holders" of the files). The latter group of actors were not exempted from compliance however: several provisions of the LIFL were directly applicable to actors that performed data processing on behalf of others.[705]

336. AFTERMATH – Several acts of implementation were adopted shortly after the enactment of the LIFL.[706] A first revision took place after 10 years,[707] but introduced only minor modifications. Substantial modifications were introduced in 1994 to regulate to processing of medical data for research purposes.[708] The act underwent major revisions in 2004 to implement Directive 95/46/EC.[709]

---

[702] E.g., as regards the consultative role of the entity charged with supervising compliance with the act (as opposed to a default licensing scheme). Compare *supra*; nrs. 233 et seq.

[703] Gesetz zum Schutz vor Miβbrauch personenbezogener Daten bei der Datenverarbeitung of 27 January 1977, *Bundesgesetblatt* 1 February 1977, I, Nr. 7, p. 201.

[704] E.g., as regards its applicability to public and private sector data processing and the duties of the "responsible keeper". Compare *supra*; nrs. 256 and nr. 267 et seq.

[705] The punitive provisions of the LIFL also did not distinguish between those processing on their own account and those processing on behalf of others. The CIL report had, however, indicated a desire not to introduce instances of vicarious criminal liability (cf. *supra*; nr. 326). As a result, one might argue that those acting "on behalf" of others might not be criminally responsible as long as they acted in accordance with the instructions issued to them.

[706] See Commission Nationale de l'Informatique et des libertés (CNIL), Premier rapport au Président de la République et au Parlement 1978-1980, *La Documentation Française*, Paris, 1980, p. 10.

[707] Loi n° 88-227 du 11 mars 1988 relative à la transparence financière de la vie politique, *J.O.* 12 March 1988, p. 3290.

[708] Loi n° 94-548 du 1 juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.* 2 July 1994, p. 25

[709] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.* 7 August 2004, p. 24.

Chapter 4 INTERNATIONAL INSTRUMENTS

1 INTRODUCTION

337. DATA CROSSES BORDERS – During the 1970s, policy makers became increasingly concerned with the international dimension of data protection.[710] Transborder flows of personal data were gradually becoming a reality to be reckoned with. Certain policymakers feared that protections offered by national laws might be circumvented by "offshoring" data processing activities.[711] Any restrictions on the international transfer of personal data, however, would disrupt free information flow and trade.[712] To address this issue, international organisations started to form working groups of experts to explore the necessities and implications of data protection at the international level.[713]

338. INTERNATIONAL INITIATIVES – Although individual accounts vary, the first international discussions on the need for data protection may be situated towards the end of the 1960's.[714] The increasingly international dimension of data flows made it imperative that certain "basic rules" be established and agreed upon at international level.[715] Data protection was discussed at various intergovernmental and non-governmental fora.[716] In the end, however, there were two international organisations which would contribute most to the development of harmonised data protection standards, namely the Organisation for Economic Cooperation and Development (OECD) and the Council of Europe.[717] The following sections will analyse the main data protection instruments adopted by both organisations.

---

[710] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 20, C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 130.
[711] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 130
[712] Id. Additional concerns related to jurisdictional conflicts resulting from discrepancies among national laws, as well issues regarding remedies and enforcement (*Ibid*, p. 130-131). See also M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 27-28
[713] G. Stadler and T. Herzog, "Data Protection: International Trends and the Austrian Example", *l.c.*, p. 6
[714] Compare e.g. F.H. Cate, "The EU Data Protection Directive, Information Privacy, and the Public Interest", *l.c.*, 431 with D. Campbell and J. Fisher (eds.), *Data transmission and privacy*, Center for International Legal Studies, Martinus Nijhoff Publishers, Dordrecht, 1994, vii and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 131-132.
[715] M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 29
[716] See C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 132-133.
[717] *Id.*

2 THE OECD GUIDELINES (1980)

2.1 ORIGIN AND DEVELOPMENT

339. ABOUT THE OECD – The Organisation for Economic Co-Operation and Development (OECD) is an intergovernmental organisation, established in 1961.[718] Its mission is to promote policies that (1) stimulate economic growth, employment, and a rising standard of living and (2) contribute to the development of the global economy and the expansion of world trade.[719] The OECD pursues this aim primarily by conducting surveys and studies; identifying and analysing the consequences of alternative policies; and then making the results of these exercises available to national policy-makers.[720] It also develops and issues recommendations to its Member countries on policy matters of common interest.[721]

340. ECONOMIC RELEVANCE – The OECD took an early interest in information processing and computerization.[722] From the 1960's onward, the OECD considered information to be an increasingly important economic asset.[723] When the first data protection laws emerged, concerns arose as to how such legislation might affect the free flow of data across borders.[724] Transborder data flows ("TBDF") were generally perceived as being beneficial to economic and social development. Any restrictions upon TBDF could impede those benefits from accruing and therefore required careful consideration.[725]

---

[718] The OECD was created by way of the Convention on the on the Organisation for Economic Co-operation and Development, Paris 14 December 1960, which entered into force on 30 September 1961 (see http://www.oecd.org/about/history, last accessed 24 October 2013). The full text of the Convention is available at available at http://www.oecd.org/general/conventionontheorganisationforeconomicco-operationanddevelopment.htm (last accessed 24 October 2013). Its initial Membership of 18 countries included European nations, together with the United States and Canada. Today, the OECD brings together 34 Member countries as well as a number of "key partner" states. See http://www.oecd.org/about/membersandpartners (last accessed 31 October 2013)

[719] Article 1 of the Convention on the Organisation for Economic Co-operation and Development.

[720] F. W. Hondius, *Emerging data protection in Europe*, o.c., p. 57.

[721] Pursuant to articles 5 and 6 of the Convention of the OECD the OECD can also take binding decisions upon its Member countries, but the number of Recommendations far outweigh the number of Decisions. See http://webnet.oecd.org/oecdacts/ for an overview of all instruments adopted by the OECD.

[722] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 136.

[723] *Id.* See also B. Godin, "The information economy: the history of a concept through its measurement, 1949-2005", *History and Technology: An International Journal* 2008, Vol. 24, n. 3, p. 256 et seq.

[724] M.D. Kirby, "Transborder Data Flows and the "Basic Rules" of Data Privacy", *l.c.*, p. 42.

[725] See also M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 8 ("*It was the potential of TBDF to occasion restrictions, regulations and even treaties within the global community of free markets and for these to impose 'barriers' on the free flow of data that attracted the interest of the OECD. Specifically, they enlivened its mission to contribute to (and defend) free flows deemed suitable to market information economies. Put bluntly, the OECD concern was that the response of European nations (and European regional institutions) to the challenges of TBDF for privacy might potentially erect legal and economic barriers against which it was essential to provide effective exceptions.*") See also OECD, "The Evolving Privacy Landscape: 30 Years After

341. PREPARATION – Between 1968 and 1974, the OECD undertook a range of studies and organised multiple seminars regarding the technological, economic and legal implications of computing.[726] In 1977, an intergovernmental Expert Group on "Transborder Data Barriers and Privacy Protection" was established.[727] According to the Terms of Reference, the mission of this Expert Group was to (1) develop guidelines on basic rules governing transborder flow and the protection of personal data and privacy with a view of facilitating harmonization and (2) investigate the legal and economic problems relating to the transborder flow of nonpersonal data.[728] The Expert Group was to carry out its activities "in close co-operation and consultation" with the Council of Europe and the European Community.[729]

---

the OECD Privacy Guidelines", *OECD Digital Economy Papers* 2011, No. 176, OECD Publishing, Paris, p. 7 and 11, available at http://dx.doi.org/10.1787/5kgf09z90c31-en (last accessed 25 October 2013).

[726] In 1968, the OECD's Committee on Science and Policy decided that the topic of "computer utilization" should be examined, leading to the subsequent establishment of a "Computer Utilization Group". The task of this group was to study the technological, economic and legal questions relating to computers and telecommunications. (C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 136). The group produced a number of studies under the series "OECD Informatics studies". In 1971, the Group commissioned a consultant report entitled "Digital information and privacy problem" (G.B.F. Niblett, "Digital information and the privacy problem", *OECD Informatics Studies*, nr. 2, 1971, OECD, Paris, 58 p.) The report explored the privacy issues related to computer usage and included a survey of regulatory responses to date. In 1974, a Data Bank Panel was established to further explore policy problems related to data banks. This Data Bank Panel organized a special seminar on the topic of "policy issues in data protection and privacy", which was attended by data protection experts from both sides of the Atlantic. (OECD, "Policy issues in data protection and privacy. Concepts and perspectives", *OECD Informatics Studies*, nr. 10, 1976, OECD, Paris, 324 p.) The 1974 seminar was followed by a larger symposium on "Transborder Data Flows and the Protection of Privacy" in 1977 (OECD, "Transborder Data Flows and the Protection of Privacy", *Information Computer Communications Policy*, nr. 1, 1979, OECD, Paris, 335 p.) See also P. Svenonius, "Address", OECD, "Policy issues in data protection and privacy. Concepts and perspectives", *OECD Informatics Studies*, nr. 10, 1976, OECD, Paris, p. 48; F. W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 58.; H.P. Gassman, "30 Years After: The Impact of the OECD Privacy Guidelines", Speech delivered at the Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP), 10 March 2010, Paris, available at www.oecd.org/sti/ieconomy/44945922.doc (last accessed 24 October 2013) and OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 9.

[727] M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 43. See also the Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, paragraph 18, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum (last accessed 25 October 2013) (hereafter: "Explanatory Memorandum"). The Expert Group was established under the OECD's Directorate for Science, Technology and Industry's Committee for Information, Computer and Communications Policy (DSTI/ICCP) (M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 7.) It was chaired by Honourable Justice Michael Kirby of Australia. (Explanatory Memorandum, paragraph 19.)

[728] M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 43.

[729] *Id.* See also Explanatory Memorandum, paragraph 19. The OECD expert group was asked to build, inter alia, on the previous and ongoing work undertaken by the Nordic Council, the Council of Europe, the European Economic Community. The aim was to bring the principles which were then emerging in these fora into an intercontinental instrument so that they could extend to other Member countries of the OECD, such as the United States, Canada, the United Kingdom, Japan, and Australia and New Zealand. (M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 7-9.) At the same time, it was also hoped that an international definition of general principles might help reduce or discourage the adoption of national legislation that would impose artificial barriers on the free flow of information. (M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 28.)

342. ADOPTION – In 1979, the Expert Group presented its draft Guidelines, together with an Explanatory Memorandum, to the Committee for Scientific and Technological Policy.[730] On 23 September 1980, the OECD Council formally adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[731] The Guidelines were expressed in the form of (an annex to) a non-binding Recommendation. The stated purpose of the Guidelines was three-fold. In first instance they sought to consolidate the basic principles of data protection among the Member countries. Complementary to this objective, the Guidelines also encouraged Member countries to remove (or avoid creating) unjustified obstacles to transborder flows of personal data. Finally, the Guidelines also encouraged Member countries to co-operate with each other during their implementation.[732]

2.2 SCOPE

343. PUBLIC AND PRIVATE SECTOR – The OECD Guidelines were to govern both public and private sector data processing (paragraph 2). In principle, no distinction was made with regards their application to either sector.[733] However, the Guidelines did recognize that exceptions could be made in the name of national sovereignty, national security and public policy.[734]

344. PERSONAL DATA – The OECD Guidelines applied only to the processing of personal data, which were defined as "*any information relating to an identified or*

---

[730] M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 43.

[731] Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data", 23 September 1980, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 28 October 2013)(hereafter: "OECD Guidelines"). This was the same month that the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was adopted. However, the Convention was not opened for ratification until 1981. (OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 12) See also *infra*; nr. 382.

[732] See the Council Recommendation accompanying the OECD Guidelines.

[733] See also A.C.M. Nugter, *o.c.*, p. 22. Paragraph 5 merely noted that "*[i]n the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation*".

[734] Even though the OECD Guidelines were expressed as a non-binding Recommendation, its drafters nevertheless considered it important to incorporate guidance with regard to potential exemptions or derogations. (Explanatory Memorandum, paragraph, 46). Paragraph 4 recognized that exceptions could be made in the name of national sovereignty, national security or public policy, but added that those exceptions should be (a) as few as possible, and (b) made known to the public. In addition, the scope of the Guidelines was limited to data which, "*because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties*" (paragraph 2). This also meant that personal data processing which obviously did not contain any risk to privacy and individual liberties could be formally exempted from any policy measures implementing the Guidelines (see paragraph 3(b)). According to the Explanatory Memorandum, "*the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (e.g. personal notebooks)*". (*Ibid*, paragraph, 43).

identifiable individual" (paragraph 1(b)).[735] In principle, any data conveying information that could be connected to a physical person, either directly (e.g., by means of a civil registration number) or indirectly (e.g., by means of an address), fell within the scope of this definition.[736]

345. AUTOMATED AND NON-AUTOMATED – The Guidelines in principle applied both to automated and non-automated data processing.[737] Neither term was explicitly defined.[738]

2.3 BASIC PROTECTIONS

346. OVERVIEW – The OECD Guidelines were divided into four substantive parts, namely (1) basic principles of national application, (2) basic principles of international application; (3) national implementation; and (4) international co-operation.

A. Basic principles of national application

347. MINIMUM STANDARDS – The first substantive part of the OECD Guidelines set forth a number of "basic rules" for the processing of personal data. These rules, which were articulated in the form of "principles", were intended as benchmarks for national policies aiming to protect privacy.[739] It is important to note, however, that the OECD Guidelines were promulgated as minimum standards, "*capable of being supplemented by additional measures for the protection of privacy and individual liberties*" (paragraph 6). This meant that national policies (or other international instruments) could introduce additional (and perhaps more restrictive) measures to protect privacy and individual liberties.[740]

348. DEGREE OF ABSTRACTION – The basic principles of national application were articulated with varying levels of detail. These differences were attributable to (a) the degree of consensus, within the Expert Group, as to how these principles should be

---

[735] Processing of data relating to legal persons thus in principle fell outside the scope of the Guidelines (see Explanatory Memorandum, paragraphs 31-33).
[736] Explanatory Memorandum, paragraph 41.
[737] *Ibid*, paragraphs 34-38. Paragraph 3(c) of the Guidelines did however grant that "*[t]hese Guidelines should not be interpreted as preventing the application of the Guidelines only to automatic processing of personal data*".
[738] According the Explanatory Memorandum, guidance for the interpretation of the concept of "automatic data processing" could be obtained from sources such as standard technical vocabularies. (*Ibid*, paragraph 36).
[739] M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 27-29.
[740] In other words, the principles contained in the OECD Guidelines provided "a floor, not a ceiling" for the protection of privacy and individual liberties. This qualification, because it was specified in the scope section of the Guidelines, applied to the Guidelines as a whole – not only to the principles of national application.

given effect, and (b) existing knowledge and experience relating to such measures.[741] Because the Guidelines were intended as a frame of reference for many different countries (who each had varying legal systems and traditions), a certain degree of abstraction was unavoidable.[742]

349. COLLECTION LIMITATION – The first principle of national application was the collection limitation principle. According to paragraph 7,

> *"[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject*."

The first part of the collection principle made clear that personal data should not be collected indiscriminately. It encouraged policy-makers to establish boundaries upon the collection of personal data, but did not specify further what these boundaries should be.[743] The second component of this principle concerned the manner in which personal was collected. It was directed against surreptitious and deceptive data collection practices.[744] Finally, paragraph 7 also made clear that, depending on the circumstances, knowledge and/or consent of the individual concerned may (or may not) be appropriate.[745]

350. DATA QUALITY – According to the data quality principle,

> *"[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."*[746]

The requirement of "relevancy" implied that the collected data should not be "more far-reaching" than was necessary to achieve the purposes of the processing.[747] The duty to

---

[741] Explanatory Memorandum, paragraph 27.

[742] By the time the Guidelines were adopted, one third of the OECD Member countries had already undertaken to regulate the processing of personal data, among which notable differences existed (for an overview see OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 8 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 57). Any attempt to consolidate and/or harmonize basic principles from these different instruments would necessarily involve a certain degree of abstraction. See also Explanatory Memorandum, paragraph 6.

[743] According the Explanatory Memorandum, such limits could relate to (1) data quality aspects, (2) the purposes of the processing, (3) the sensitivity of data, (4) the type data controller or (5) civil rights concerns. (Explanatory Memorandum, paragraph 51.)

[744] Explanatory Memorandum, paragraph 52.

[745] The Explanatory Memorandum indicated that "*knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement […] On the other hand, […] there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary*." (*Id.*) For a discussion of how this principle was implemented in other national and international instruments see M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 49-50.

[746] Paragraph 8 of the Guidelines.

[747] Explanatory Memorandum, paragraph 53.

maintain data accuracy, supplement data, or to ensure it remained up-to-date was likewise to be assessed in light of the purposes pursued.[748]

351. PURPOSE SPECIFICATION – The purpose specification principle (paragraph 9) was closely associated with its two surrounding principles, namely the data quality principle and the use limitation principle.[749] Paragraph 9 provided that "*the purposes for which personal data are collected should be specified not later than at the time of data collection*". Any subsequent use of these data was to be limited to the fulfilment of those purposes – or at least be "compatible" with them.[750] In other words, specification of purpose made it possible to evaluate compliance, not only with the data quality principle (paragraph 8), but also with the use limitation principle (paragraph 10).

352. USE LIMITATION – Paragraph 10 stated that

> *"Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:*
>
> *a) with the consent of the data subject; or*
>
> *b) by the authority of law*".

The use limitation principle built further upon the purpose specification principle: the purposes specified prior to collection of personal data in principle determined how those data could be used. However, paragraph 10 also indicated that a deviation of purpose might be permissible in two instances, namely (a) where the individual concerned provided his or her consent or, (b) where the new use was authorized by law.[751]

353. SECURITY SAFEGUARDS – The security safeguards principle stipulated that personal data should be protected, by reasonable security measures, against "*loss or unauthorised access, destruction, use, modification or disclosure of data*" (paragraph 11). According to the Explanatory Memorandum, such security measures could be either of a physical (e.g. door locks), organisational (e.g., confidentiality obligations) or informational nature (e.g., enciphering).[752]

354. OPENNESS – The openness principle (paragraph 12) was formulated in relatively abstract terms. According to this principle,

---

[748] According to the Explanatory Memorandum, this "'*purpose test' will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating".* (*Id.*)

[749] Explanatory Memorandum, paragraph 54.

[750] Explanatory Memorandum, paragraph 54. It is interesting to note that the Explanatory Memorandum also infers from this principle that "*when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.*") (*Id.*)

[751] See also Explanatory Memorandum, paragraph 55.

[752] Explanatory Memorandum, paragraph 56.

> *"[t]here should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*"

This principle implied that individuals should be in a position to obtain information about the collection, storage and use of personal data, without unreasonable effort or cost.[753] However, the Guidelines themselves remained agnostic as to how such openness was to be realized in practice.[754]

355. INDIVIDUAL PARTICIPATION – The principle of individual participation was generally considered as one of the most important privacy safeguards.[755] As a result, it was articulated in rather direct and specific terms. Paragraph 13 of the Guidelines provided that data subjects should have a right (1) to access their data (i.e., to receive communication of data relating to him in a reasonable manner) and (2) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

356. ACCOUNTABILITY – The principle of accountability was of central importance to the OECD Guidelines. Paragraph 14 provided that:

> "*A data controller should be accountable for complying with measures which give effect to the principles stated above*".

The objective of this principle was two-fold. First, it served to assign (primary) responsibility for compliance to the "data controller".[756] Secondly, this principle encouraged Member countries to institute mechanisms which ensure that data controllers are held answerable in case this responsibility is not met.[757] The Explanatory Memorandum to the Guidelines elaborated upon the rationale and implications of this principle as follows:

> *"The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this*

---

[753] Explanatory Memorandum, paragraph 57.

[754] According to the Explanatory Memorandum, openness could be realized inter alia by "*regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies*" (*Ibid*, paragraph 57.)

[755] *Ibid*, paragraph 58.

[756] See also M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 60. The "data controller" was defined by paragraph 1(a) as "*a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*". See also *infra*; nr. 364.

[757] J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 53.

obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau."[758]

The Guidelines themselves did not prescribe to whom the controller should be accountable, nor did it prescribe any specific accountability mechanisms. The Memorandum merely indicated that "*accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.*"[759]

B. Basic principles of international application

357. PURPOSE – The main driver behind the development of the OECD Guidelines was, as mentioned earlier, the concern that privacy laws might create artificial barriers to the free flow of data.[760] In an attempt to mitigate this risk, paragraphs 15-18 of the Guidelines called upon Member countries to (a) remain mindful of each other's interests in relation to the processing of personal data; (b) ensure the security and continuity of transborder data flows; and (c) avoid unnecessary restrictions upon transborder data flows.

358. MUTUAL CONSIDERATION – According to paragraph 15,

"Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data."

This provision sought to foster mutual consideration, by Member countries, for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents.[761] It was directed, first and foremost, against national policies which might facilitate attempts to circumvent or violate protective legislation of other Member countries.[762] In addition, it implicitly encouraged Member countries to consider the need to adapt their rules and practices governing the processing of data to the particular circumstances which might arise when foreign data and data on non-nationals were involved.[763]

359. SECURITY AND CONTINUITY OF TBDF – Paragraph 16 called upon Member countries to take appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, remained "uninterrupted and secure". This provision intended to encourage Member countries to protect TBDF against

[758] Explanatory Memorandum, paragraph 62.
[759] *Id*.
[760] Cf. *supra*; nr. 340.
[761] Explanatory Memorandum, paragraph 63.
[762] *Ibid*, paragraph 64. The reference to "re-export" was inserted to encourage Member countries "*to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent*" (*Id.*)
[763] Explanatory Memorandum, paragraph 65.

unauthorized access, loss of data and similar events, as well as to ensure the availability of channels and installations necessary to carry out the uninterrupted exchange of data.[764]

360. AVOIDING UNNECESSARY RESTRICTIONS – Paragraph 17 recognized that restrictions upon TBDF might be legitimate in certain instances. Specifically, such restrictions would be legitimate when (a) the other Member country did not yet substantially observe the Guidelines or (b) the re-export of such data would circumvent its domestic privacy legislation. Member countries could also legitimately impose restrictions in respect of certain categories of personal data for which the other Member country provided no equivalent protection (paragraph 17, *in fine*). Paragraph 18 asked Member countries to ensure that such restrictions did not exceed that which was necessary for the protection of privacy.[765]

C. National implementation

361. A GENERAL FRAMEWORK – Paragraph 19 provided a general outline of how the Guidelines might be implemented at national level. Recognizing that this implementation was bound to vary according to different legal systems and traditions, this paragraph merely attempted to signal, in broad terms, what kind of "national machinery" was envisaged for putting the Guidelines into effect.[766]

362. ELEMENTS – According to paragraph 19, the following elements merited consideration when implementing the Guidelines: (a) the adoption of appropriate legislation; (b) the promotion of self-regulation; as well as (c) the administration of sanctions and remedies in cases of failure to comply with measures implementing the Guidelines. In addition, paragraph 19 also envisaged "reasonable means for individuals to exercise their rights" and measures to prevent "unfair discrimination against data subjects".[767]

D. International Co-operation

363. ELEMENTS – The final section of the OECD Guidelines specified a number of areas in which Member countries were encouraged to co-operate further, namely:

a) exchange of information regarding the implementation of the Guidelines[768];

[764] Explanatory Memorandum, paragraph 66.
[765] See also Explanatory Memorandum, paragraph 68.
[766] Explanatory Memorandum, paragraph 69. This aspect of "flexible implementation" is considered to have been key to the success of the OECD Guidelines. See M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 11.
[767] See Explanatory Memorandum, paragraph 70.
[768] Paragraph 20 of the Guidelines. See also Explanatory Memorandum, paragraph 71-72.

b) the development of compatible procedures for TBDF[769];

c) procedural and investigative matters, particularly among data protection authorities and entities dealing with information policy issues[770]; and

d) the development of conflict of laws rules[771].

2.4 ALLOCATION OF RESPONSIBILITY AND RISK

364. FORMAL DEFINITION – The OECD Guidelines formally defined the actor which should be responsible for ensuring compliance with its provisions. The responsible actor was the "data controller", which was defined by paragraph 1(a) as

> "*a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*."[772]

A number of general criteria can be extrapolated from this definition, each of which shall be elaborated over the following paragraphs.

365. A PARTY – Under the OECD Guidelines, a data controller could be a natural or legal person, public authority, agency or any other body.[773]

366. DECISION-MAKING POWER – The data controller was the actor who, according to domestic law, was "*competent to decide*" about the collection and use of personal data. A first constitutive element of the data controller concept was thus a competency to exercise decision-making power. The reference to "according to domestic law" underlined that Member countries retained discretion in developing additional criteria for determining such competency.[774]

367. CONTENTS AND USE – The second constitutive element of the data controller concept concerned the object of its decision-making power, namely the "contents and use" of personal data. According to the Explanatory Memorandum, the data controller was the actor who "*decide[d] about data and data processing activities*".[775] Arguably, this encompassed various aspects of the processing, such as the types of data to be collected, the purposes of the processing, which entities would have access to the data, the logic of

---

[769] *Id.*
[770] Paragraph 21 of the Guidelines. See also Explanatory Memorandum, paragraph 73.
[771] Paragraph 22 of the Guidelines. See also Explanatory Memorandum, paragraph 74-76.
[772] Paragraph 1(a) of the OECD Guidelines (emphasis added).
[773] Explanatory Memorandum, paragraph 40.
[774] P.H. Patrick, "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines", *Jurimetrics Journal* 1980-1981, Vol. 21, p. 410.
[775] Explanatory Memorandum, paragraph 62.

the processing, etc.[776] In other words: the data controller was the actor that decided about the "input" of the processing as well as how this input was to be applied.

368. CUI BONO – According to the Explanatory Memorandum, the data controller was the party for whose benefit the processing of personal data is being carried out.[777] This aspect was also reflected implicitly in paragraph 1(a), which stated that a party might be considered a data controller "*regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*" (emphasis added). The reference to "on his behalf" suggested that the processing was undertaken to serve the controller's interests.

369. EXCLUDED ENTITIES – The Explanatory Memorandum stated that certain types of actors, although they might be involved in the processing of data, should not be considered data controllers.[778] Specifically, the data controller concept reportedly excluded

> "*(a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc.*"[779]

This portion of the Explanatory Memorandum made clear that not every actor with decision-making power over the processing should necessarily be considered a data controller. It also made clear that an actor might be engaged in the processing of personal data without acting as a data controller.[780]

---

[776] This interpretation is corroborated by the latter portion of paragraph 40 of the Explanatory Memorandum, which indirectly paraphrases the controller's decision-making power as being entitled to decide "*what activities should be carried out and for what purposes*" and "*what data should be stored, who should be able to use them, etc*".

[777] Explanatory Memorandum, paragraph 62.

[778] *Ibid*, paragraph 40.

[779] *Id*.

[780] The exclusion of "service bureaux" from the data controller concept echoes one of the recommendations submitted to the 1977 OECD symposium on Transborder Data Flows and the Protection of Privacy. Specifically, it was recommended that a distinction be maintained between, on the one hand, the "*use* of data" and the "*processing* of data" and, on the other hand, between the organisation or individual "on whose behalf and under whose direction" data processing work is done (the "*beneficial user*") and the individual or organisation on whose computing systems processing is carried out (the "*agency*"). The former should be subject to applicable data protection laws, whereas the latter should be capable of providing a level of security appropriate to the level of sensitivity of the data. See A.A. Benjamin, "Privacy and Computers", in OECD, *Transborder Data Flows and the Protection of Privacy*, *o.c.*, p. 175-176. It is worth noting the affiliation of the author, i.e. the UK Computing Services Association. The contribution by P.C. Onstad, Chairman of the Association of Data Processing Services, followed a similar vein: see P.C. Onstad, "Data Processing Services and Transborder Data Flows", in in OECD, *Transborder Data Flows and the Protection of Privacy*, *o.c.*, p. 180 (comparing data processing services to a "safety box"

370. GENESIS OF THE "DATA CONTROLLER" CONCEPT – The term "data controller" had not figured in any of the national laws adopted prior to the Guidelines. While several of those laws formally defined a "responsible actor", none of them used a term which was etymologically related to the word "controller". How this term came to be introduced is therefore somewhat uncertain. However, the limited documentation that exists regarding the introduction of this concept provides some indication. Speaking at an OECD symposium in 1977, F.W. Hondius, a representative of the Directorate of Legal Affairs of the Council of Europe, commented on the difficulties in developing a common understanding of key concepts as follows:

> *"The main difficulty we encountered in preparing this draft was, to use a computer term, to create interfaces between widely different concepts of the various national legal systems. […] But we found it worth the effort, after having made an analytical survey of the key concepts of national legislation, to try our hand at international standards. Mr. Benjamin will be pleased to recognize, for example, his 'beneficial user' concept, which is disguised in our text as 'controller of the record', a clumsy English rendering of the marvellous French expression 'maître du fichier'."*[781]

It seems reasonable to conclude, on the basis of this text, that the term "controller of the file" emerged in the course of the discussions surrounding the preparation of Convention 108 and the OECD Guidelines.[782] This term was not, however, created *de novo*. Its inspiration seems to have stemmed from computer science literature, in particular the writings of Rein Turn.[783]

371. ENTITIES "ACTING ON BEHALF OF" – The OECD Guidelines allocated "ultimate" responsibility for compliance with the data controller.[784] They did not assign any responsibility to entities acting on behalf of a data controller. The Explanatory

---

leased by a bank to the customer; whereby the customer is totally responsible and "in complete control" of all input and output to the box; whereas the bank can at most assume responsibility for the physical security of the box).

[781] F.W. Hondius, "The Action of the Council of Europe with regard to International Data Protection", in OECD, "Transborder Data Flows and the Protection of Privacy", *o.c.*, p. 260 (emphasis added). See also supra; footnote 780.

[782] The Committee of Experts tasked with preparing Convention 108 also comprised participants from countries outside of Europe, as well as members of the OECD Expert Group on Transborder Data Barriers and Privacy Protection. The suggestion to use the term "controller" may therefore have originated from either forum.

[783] In his 1975 book, Hondius noted that Rein Turn used the term "controller" to refer to what he would refer to as the "user" of a data bank (see F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 101-103). Turn had also used the term "controller" in his contribution to the 1974 OECD seminar on Policy issues in data protection and privacy (see R. Turn, "Data security: costs and constraints" in OECD, *Policy issues in data protection and privacy*. *Concepts and perspectives*, *o.c.*, p. 244 et seq.), as well as in anterior publications (dating back at least to 1967). See e.g. H.E. Peterson and R. Turn, "System implications of information privacy", in *Proceeding AFIPS '67,* (Spring) Proceedings of the April 18-20, 1967, spring joint computer conference, ACM, New York, p. 293. Turn's use of the term "controller" displayed strong conceptual similarity with the terms "data controller" and "controller of the file". In his contribution to 1974 OECD seminar, for example, he defined the "controller" as "*(an agency) with authority over the data-base system, which specifies the population of subjects, type of data collected, and the protection policies*". (R. Turn, "Data security: costs and constraints", *l.c.*, p. 244).

[784] Explanatory Memorandum, paragraph 40.

Memorandum noted, however, that Member countries remained free to develop "*more complex schemes of levels and types of responsibilities*" when implementing the Guidelines.[785] For example,

> *"[…] nothing in the Guidelines prevents service bureaux personnel, "dependent users" […] and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (cf. Paragraph 19 of the Guidelines)."*[786]

As we have seen earlier, the privacy laws of Hesse, Sweden and France all allocated certain responsibilities upon entities acting "on behalf of" the "responsible" entity, whether they were acting in the capacity of a service provider or as an employee.[787] For the most part, their responsibilities were limited to (a) duties of confidentiality; (b) an obligation to ensure security of processing; as well as (c) a general duty to co-operate with supervisory authorities.[788]

372. ROLE OF THE ACCOUNTABILITY PRINCIPLE – Within the OECD Guidelines, the principle of accountability served as a vehicle to assign responsibility for compliance "*with measures which give effect to the principles*".[789] Rather than limiting the scope of the Guidelines *ratione personae*, the drafters chose to introduce an additional principle as a means of assigning responsibility. This choice was reflective of the fact that the OECD Guidelines were directed towards Member countries, rather than being directly applicable to data controllers. As noted by Kirby, the principle of accountability

> *"sought to identify a duty-bearer so that there would be no doubt as to who had the obligation to comply with the Guidelines in particular cases. The passive voice and subjunctive mood of hortatory language, common in international instruments, can sometimes weaken the power of their instruction. The value of the 'accountability*

---

[785] Explanatory Memorandum, paragraph 40.

[786] *Ibid*, paragraph 62. For a detailed discussion of the "processing services" and "data services" offered by "(computer) service bureaux" at the time see J. Bing, P. Forsberg and E. Nygaard, "Legal problems related to transborder data flows", in OECD, *An Exploration of Legal Issues in Information and Communication Technologies*, Information Computer Communication Policy nr. 8, Paris, OECD, 1983, p. 129-131.

[787] Cf. *supra*; nr. 244 (Hesse); nr. 283 (Sweden) and nr. 329 (France).

[788] *Id.* It is worth noting that the federal data protection act of (West) Germany (1977) imposed a more comprehensive set of obligations upon the "data protection representative" ("*Datenschutzbeauftragten*"), who acted as a "responsible person" within an organisation that had decided to process personal data. See paragraph 29 of the Act on the Protection against the Misuse of Personal Data in Data Processing ("*Gesetz zum Schutz vor Missbrach Peronenbezogener Daten bei der Datenverarbeitung – Bundesdatenshutzgesetz*") of 27 January 1977 (*Bundesgesetzblatt* Nr. 7 of 1 February 1977, Part I (Teil I), p. 201). See also M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 61. For a critical evaluation see S. Simitis, "Establishing Institutional Structures to Monitor and Enforce Data Protection", in OECD, "Policy issues in data protection and privacy. Concepts and perspectives", *OECD Informatics Studies*, *o.c.*, p. 85-86.

[789] Cf. *supra*; nr. 356. Kirby has noted that the accountability principle was to some extent an OECD novelty: see M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 10 ("*The OECD Guidelines added the 'accountability principle' (para.14). That principle had not been included, as such, in the earlier European work."*) As noted by the same author, the principle of accountability had already figured in the 1974 US Privacy Act: see M.D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *l.c.*, p. 38.

principle' is that it permits elaboration and identification of the duty-bearer. This is important for the effective implementation of the Guidelines."[790]

As indicated earlier, the principle of accountability also served a second purpose, namely as the articulation of a governance principle.[791] It postulated that accountability mechanisms should be in place to ensure that data controllers would be answerable in case of failure to comply with measures giving effect to the Guidelines. While the Guidelines did not specify precisely which accountability mechanisms should be in place, it signalled the importance of such mechanisms for the practical effectiveness of the Guidelines.

373. ALLOCATION OF RISK – The Guidelines did not specify which mechanisms of civil or criminal liability Member countries should introduce. Paragraph 19(d) merely encouraged Member countries to

"provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three."

As indicated earlier, the OECD Guidelines recognized that Member countries had varying regulatory cultures and traditions; and thus might employ different means to pursue effective enforcement. In relation to the accountability principle, the Explanatory Memorandum noted this principle "*refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance*".[792]

2.5 CONCLUSION

374. BUILDING ON PREDECESSORS – The OECD Guidelines represented the first internationally agreed statement of core privacy protection principles.[793] The Guidelines were not, however, developed from scratch. The drafters of the Guidelines "*did not set out to reinvent the wheel or needlessly to alter sensible approaches that had been adopted by [their] predecessors*".[794] The chairman of the Expert Group, Michael Kirby, has noted the input received from academic writing, as well as from governmental reports available at the time, such as those developed in the United States, the United Kingdom and France.[795] In addition, Mr. Kirby also noted the input provided by Frits Hondius, representative of the Council of Europe, who assisted them in drawing on the Council's work as they "translated that work into an inter-continental context".[796]

375. A CRAFTY COMPROMISE – The OECD Guidelines have been dubbed "a carefully crafted compromise"; being able to cater to the range of views held by the members of

[790] M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 10.
[791] Cf. *supra*; nr. 372.
[792] Explanatory Memorandum, paragraph 70.
[793] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 2.
[794] M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 10.
[795] *Id.*
[796] *Id.*

the Expert Group.[797] The success of the OECD Guidelines has been attributed in part to their flexible implementation, which recognized that Member countries would follow their own regulatory cultures.[798] By incorporating a certain degree of abstraction, the OECD managed to forge a consensus among experts from both sides of the Atlantic, who at times hold very diverging views on how to best implement privacy protections.

376. ALLOCATION OF RESPONSIBILITY AND RISK – The OECD Guidelines, together with its accompanying Memorandum, foreshadowed a number of developments in data protection regulation. First, the Guidelines placed the primary responsibility for compliance on the "data controller". This term, or minor variations thereof, would be echoed in subsequent national and international instruments. Second, the Guidelines indicated that the data controller's responsibilities should not necessarily end once data is transferred to another party. Specifically, the Guidelines suggested that a data controller should remain accountable in relation to processing carried out by a third party on its behalf. At the same time, they also recognized that there may be instances in which it is appropriate for a service bureau, that processes data on behalf of a data controller, to also be held accountable for certain aspects related to the processing. Finally, the accountability mechanisms suggested by the Guidelines, namely legal sanctions and codes of conduct, still remain relevant today.[799]

377. AFTERMATH – After the Guidelines were adopted, the OECD promulgated a number of additional declarations and recommendations concerning privacy and transborder data flows. In 1985, the governments of the OECD Member countries adopted the "Declaration on Transborder Data Flows"[800], which concerned the promotion of both personal and non-personal data flows. In 1998, the "Declaration on the Protection of Privacy in Global Networks"[801] was adopted, which encouraged Member countries to take certain measures towards achieving effective implementation of the Guidelines. In 2007, the OECD issued its "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy"[802], which represented a commitment on the part of Member countries to promote closer co-operation among privacy enforcement authorities.[803] The Guidelines themselves were formally revised in

---

[797] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 10.
[798] M. Kirby, "The history, achievement and future of the 1980 OECD guidelines on privacy", *l.c.*, p. 11.
[799] J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 54-55.
[800] OECD, *Declaration on Transborder Data Flows*, 11 April 1985, Paris, OECD, available at http://www.oecd.org/internet/ieconomy/declarationontransborderdataflows.htm (last accessed 5 November 2013).
[801] OECD, Declaration on the Protection of Privacy in Global Networks, adopted at the Ottawa Ministerial Conference 7-9 October 1998, adopted as OECD Council Resolution on 19 October 1998, available at http://www.oecd.org/sti/ieconomy/1840065.pdf (last accessed 5 November 2013).
[802] OECD, *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 2007, OECD, Paris, available at www.oecd.org/dataoecd/43/28/38770483.pdf (last accessed 5 November 2013).
[803] OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 33

2013.[804] While this revision did not affect the core principles of the Guidelines, it elaborated further upon a number of aspects, including the development of accountability mechanisms.

[804] OECD, "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data", C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last accessed 5 November 2013).

3 CONVENTION 108 (1981)

3.1 ORIGIN AND DEVELOPMENT

378. ABOUT THE COUNCIL OF EUROPE – The Council of Europe (CoE) is an intergovernmental organisation, established in 1949.[805] Its mission is to achieve "a greater unity" between its member States in order to advance their (a) common ideals and principles and (b) economic and social progress.[806] The promotion of human rights and fundamental freedoms is particularly central to the mission of the CoE.[807] The CoE pursues its objectives through discussion of questions of common concern, by concluding agreements and by undertaking common action.[808] Perhaps the most notable achievement of the CoE is the European Convention on Human Rights[809] (ECHR) (1950), the implementation and enforcement of which has been overseen by the European Court of Human Rights since 1959.[810]

379. HUMAN RIGHTS' RELEVANCE – The efforts of the CoE in the field of data protection were born of the recognition that certain technological developments posed a threat to the rights and freedoms of individuals, in particular their right to privacy.[811] Of particular concern were "*newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda*".[812]

380. EARLY INITIATIVES – In 1968, the Parliamentary Assembly of the CoE adopted a Recommendation concerning human rights and modern scientific and technological

---

[805] The Council of Europe was created by way of the Treaty on the Statute of the Council of Europe, London, 5 May 1949 which entered into force 3 August 1949. The full text of the convention is available at http://conventions.coe.int/Treaty/en/Treaties/Html/001.htm (last accessed 6 November 2013). The initial membership of the CoE included 10 European States (Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the United Kingdom). Today, the Council of Europe comprises 47 member states, 28 of which are members of the European Union. See http://www.coe.int/nl/web/portal/47-members-states (last accessed 27 April 2016).

[806] Article 1(a) of the Statue of the Council of Europe.

[807] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 63. See Article 1(b) of the Statue of the Council of Europe. See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 133.

[808] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 63. See Article 1(b) and 1(d) of the Statue of the Council of Europe.

[809] Council of Europe, European Convention of Human Rights, 4 November 1950, available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (last accessed 8 November 2013).

[810] See http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (last accessed 6 November 2013).

[811] See Parliamentary Assembly of the Council of Europe, "Recommendation 509 (1968) concerning Human rights and modern scientific and technological developments", 31st January 1968 (16th Sitting), available at http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=14546&lang=en (last accessed 8 November 2013), at paragraph 3.

[812] *Id.*

developments.[813] This Recommendation called for a study to examine whether member States' laws and the ECHR sufficiently protected the right to privacy "*against violations which could be committed by the use of modern scientific and technical methods*".[814] In 1970, a preliminary report was produced which answered this question in the negative.[815] Seeing as the increased usage of computers was at the focus of concern, the decision was made to concentrate further study efforts on electronic data banks.[816] In 1971, the Committee of Experts which was set up for that purpose noted that many governments were already considering regulation of computer usage in order to protect privacy and advocated for concerted action.[817] In order to facilitate the development of common European norms, the Committee developed two resolutions containing basic principles with regard to the gathering, storing, processing and dissemination of personal data by means of computers.[818] The first resolution, adopted by the Committee of Ministers in 1973, concerned the protection of individuals' privacy vis-à-vis electronic data banks in the private sector.[819] The second resolution, adopted in 1974, called for the application of similar principles to the public sector.[820]

381. PREPARATION – In 1976, the Committee of Ministers tasked a Committee of Experts on Data Processing "*to prepare a convention for the protection of privacy in relation to data processing abroad and transfrontier data processing*".[821] This decision was motivated by the recognition that data flows were becoming increasingly transnational in nature. Concerned that national legislators might otherwise erect

---

[813] *Id.* For a more detailed account of the discussions that took place see P. Vegleris, "Preadvies", in X., *Privacy en de rechten van de mens. Handelingen van het Derde Internationaal Colloquium over het Europees Verdrag tot Bescherming van de Rechten van de Mens*, Leuven, Acco, 1974, p. 337-342 and A.C. Evans, "Data Protection Law", *The American Journal of Comparative Law* 1981, Vol. 29, No. 4, p. 572.

[814] Recommendation 509 (1968), at paragraph 8.1. See also F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 65.

[815] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 65; A.C. Evans, "Data Protection Law", *l.c.*, p. 573; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 133. One of the main reasons for this conclusion was the finding that the European Convention of Human Rights did not offer sufficient protection to individuals in relation to other private parties. (F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 65.)

[816] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 66 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 133-134.

[817] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 66.

[818] *Ibid*, p. 68.

[819] Committee of Ministers of the Council of Europe, "Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector", 26 September 1973 (224th meeting of the Ministers' Deputies), available at http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (last accessed 8 November 2013).

[820] Committee of Ministers of the Council of Europe, "Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector", 20 September 1974 (236th meeting of the Ministers' Deputies), available at http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (last accessed 8 November 2013).

[821] Explanatory Report accompanying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS. 108, paragraph 13, available at http://conventions.coe.int/treaty/en/Reports/Html/108.htm (last accessed 8 November 2013) (hereafter: "Explanatory Report").

barriers to the free flow of information, the development of an internationally binding instrument was deemed necessary.[822] It is worth noting that experts from the Asia-Pacific region (Australia, Canada, Japan), the United States, the European Communities and the OECD participated in the work of the Expert Committee.[823]

382. ADOPTION – The draft text of the Convention was finalized in April of 1980.[824] It was subsequently adopted by the Committee of Ministers on 17 September 1980.[825] The *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ("Convention 108") was opened for signature on 28 January 1981.[826] The five ratifications, which were necessary before the Convention could enter into force, were received on 1 October 1985.[827]

3.2 SCOPE

383. PUBLIC AND PRIVATE SECTOR – Pursuant to article 3(1), Parties to Convention 108 were obliged to apply its provisions to "*automated personal data files and automatic processing of personal data in the public and private sectors*". The provisions of the Convention thus in principle applied equally to public and private sector activities. However, the Convention also recognized that exceptions could be made in the name of State security, public safety, monetary interests, or the suppression of criminal offences.[828]

384. PERSONAL DATA – Convention 108 only applied to the automated files or automatic processing involving personal data, which were defined by article 2(a) as "*any information relating to an identified or identifiable individual ('data subject')*". According to the Explanatory Report, the term "identifiable" referred only to situations in which

---

[822] G. Buquicchio, "The work of the Council of Europe in the field of data protection", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, p. 230.
[823] *Id.* See also Explanatory Report, paragraph 15.
[824] Explanatory Report, paragraph 17.
[825] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 135; R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 321.
[826] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", ETS. 108, Strasbourg, 28 January 1981, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (last accessed 8 November 2013) (hereafter: "Convention 108").
[827] C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 135. See also article 22 Convention 108.
[828] Article 9 enabled the Parties to Convention 108 to limit the effect of several of its provisions. Specifically, the Convention allowed exceptions to the provisions of article 5 (data quality), 6 (special categories of data) and 8 (data subject rights); provided such derogations were provided for by law and constituted a necessary measure in a democratic society. Moreover, such restrictions needed to serve the interests of (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences or (b) protecting the data subject or the rights and freedoms of others. Restrictions on the exercise of certain data subject rights could also be provided with respect to automated personal data files used for statistics or for scientific research purposes if there was obviously no risk of an infringement of the privacy of the data subjects (article 9(3)).

the individual could be identified with relative ease (excluding situations where individuals could only be identified by means of very sophisticated methods).[829]

385. AUTOMATED DATA FILES & AUTOMATIC PROCESSING – The term "automated data file" was defined as "*any set of data undergoing automatic processing*" (article 2(b)). It was intended to cover

> *"not only data files consisting of compact sets of data, but also sets of data which are geographically distributed and are brought together via computer links for purposes of processing*".[830]

The term "automatic processing" included operations such as "*the storage of data, the carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination*"; provided such operations were carried out in whole or in part by automated means (article 2(c)).[831] Non-automated processing of personal data thus in principle fell outside the scope of Convention 108. However, article 3(2)c recognized Parties' ability to extend similar protections to personal data files which were not processed automatically.

3.3 BASIC PROTECTIONS

386. OVERVIEW – Convention 108 was comprised of three main parts: (1) substantive law provisions in the form of basic principles; (2) special rules on transborder data flows; and (3) mechanisms for mutual assistance and consultation between the Parties.[832]

A. Basic principles for data protection

387. MINIMUM STANDARDS – Chapter II of Convention 108 set forth a number of "basic principles for data protection". These principles were designed to protect individuals' rights and fundamental freedoms with regard to the automatic processing of their personal data (article 1). It is important to note, however, that these "basic principles" of Convention 108 were promulgated as minimum standards. Every Party remained free to grant data subjects a wider measure of protection than was stipulated in the Convention (article 11).[833]

---

[829] Explanatory Report, paragraph 28. Processing of data relating to legal persons thus in principle fell outside the scope of Convention 108. However, article 3(2)b recognized Parties' ability to extend similar protections to "*groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality*", subject to the submission of a declaration to the Secretary General of the Council of Europe.
[830] Explanatory Report, paragraph 30.
[831] See also Explanatory Report, paragraph 31.
[832] Explanatory Report, paragraph 18.
[833] See also Explanatory Report, paragraph 61.

388. NATURE – While Convention 108 was a legally binding instrument, it was not designed to be self-executing. This meant that it did not intend to procure rights to individuals directly.[834] Instead, the Convention obliged each Party to take the necessary measures in its domestic law to give effect to the Convention's basic principles (article 4). Such measures could take different forms, depending on the depending on the legal and constitutional system of the State concerned (e.g., laws, regulations, administrative guidelines).[835] However, legally binding measures were considered necessary to ensure full compliance with the Convention.[836]

389. DATA QUALITY – According to article 5, personal data undergoing automatic processing needed to be

a) *"obtained and processed fairly and lawfully;*
b) *stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
c) *adequate, relevant and not excessive in relation to the purposes for which they are stored;*
d) *accurate and, where necessary, kept up to date;*
e) *preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."*

This provision consolidated the basic principles of data protection as introduced in earlier CoE resolutions and national data protection laws.[837]

390. SPECIAL CATEGORIES OF DATA – Contrary to the OECD Guidelines, Convention 108 did identify several types of data for which additional protection was required. The Explanatory Report reasoned that

> "*[w]hile the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests*."[838]

---

[834] Explanatory Report, paragraph 38.
[835] Explanatory Report, paragraph 39.
[836] *Id.* (noting that *"binding measures may usefully be reinforced by measures of voluntary regulation in the field of data processing, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the convention."*)
[837] Explanatory Report, paragraph 40. Seeing as these principles, save for certain nuances, bear a close resemblance to those contained in the OECD Guidelines, the reader may wish to consult the earlier discussion of the OECD privacy principles: cf. *supra*; nrs. 347 et seq. For a more detailed comparison between the provisions of Convention 108 and the OECD Guidelines see P.H. Patrick, "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines", *l.c.*, p. 405-420; J. Bing, "The Council of Europe Convention and the OECD Guidelines on Data Protection", *Michigan Yearbook of International Legal Studies* 1984, Vol. 5, p. 271-303 and P. Kayser, *La protection de la vie privée. Protection du secret de la vie privée*, *o.c.*, p. 362-364.
[838] Explanatory Report, paragraph 43.

The sensitive categories of data included personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and personal data relating to criminal convictions.[839] Such data could not be processed automatically unless domestic law provided for appropriate safeguards (article 6).

391. DATA SECURITY – Article 7 provided that

> *"appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."*

Which security measures were "appropriate" would depend *inter alia* on the risks presented, the specific function of the file, as well as the existing state of the art of data security methods and techniques.[840]

392. SAFEGUARDS FOR DATA SUBJECTS – Article 8 provided for a number of "safeguards for data subjects", designed to encourage the creation of subjective rights for data subjects.[841] These rights would enable individuals to obtain:

- knowledge about the existence of an automated data file;
- knowledge about the contents of the information, if any, stored about data subjects in a file;
- rectification of erroneous or inappropriate information;
- a remedy if any of the previous elements are not respected.[842]

B. Transborder data flows

393. PURPOSE – A main driver behind Convention 108, in addition to privacy concerns, was the fear that national privacy laws might erect barriers to the free flow of information among contracting parties. Article 12 attempted to mitigate this risk by limiting the instances in which Parties to Convention 108 might prohibit or otherwise restrict transborder flows of personal data.

394. FREE FLOW AND LEGITIMATE RESTRICTIONS – In principle, Parties to Convention were prohibited from restricting, for the sole purpose of protecting privacy,

[839] For more information regarding these data types see Explanatory Report, paragraphs 44-48.
[840] Explanatory Report, paragraph 49.
[841] Explanatory Report, paragraph 50. Article 8 expressed them in the form of "safeguards" which Contracting States were to offer in view of the non-self-executing character of the convention (*id.*).
[842] Explanatory Report, paragraph 50. Similar to the OECD Guidelines, the Convention recognized that Member States might implement these safeguards in various ways. For more information see paragraphs 50-54 of the Explanatory Report.

transborder flows of personal data going to the territory of another Party (article 12(2)). Nevertheless, each Party remained entitled to derogate from this rule (article 12(3)):

a) *"insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;*

b) *when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph*."[843]

C. Mutual Assistance

395. ELEMENTS – Chapter IV of Convention 108 specified a number of areas in which Parties were to render each other mutual assistance, namely:

a) exchange of information regarding the implementation of the Convention as well as any factual information to specific automatic processing carried out in its territory[844]; and

b) assistance to data subjects resident abroad.[845]

3.4 ALLOCATION OF RESPONSIBILITY AND RISK

396. FORMAL DEFINITION – Convention 108 contained a formal definition of the entity that would be responsible for ensuring compliance with its provisions. The responsible entity was the "controller of the file", which was defined by article 2(d) as:

> "*the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them*."[846]

397. ANY BODY – Under Convention 108, a controller could be a natural or legal person, public authority, agency or any other body.

398. DECISION-MAKING POWER – The controller of the file was the party who, according to national law, was "*competent to decide*" about the automated data file. A first constitutive element of the data controller concept was thus the authority to

[843] See also Explanatory Report, paragraphs 62-70.
[844] Article 13 Convention 108. See also Explanatory Report, paragraphs 71-76.
[845] Article 14 Convention 108. See also Explanatory Report, paragraphs 77-78. Articles 15-17 further regulated the modalities of requests for assistance.
[846] Article 2(d) of Convention 108 (emphases added).

exercise decision-making power. The reference to "according to national law" indicated that national laws might contain additional criteria for determining such competency.[847]

399. PURPOSE, CATEGORIES OF DATA & OPERATIONS – The second constitutive element of the "controller of the file" concept concerned the object of its decision-making power. The controller of the file was understood to have decision-making power over the following three elements:

- the purpose of the automated data file;
- the categories of personal data that will be stored;
- the nature of the operations applied to those data.

400. EXCLUDED ENTITIES – The Explanatory Report indicated that the concept of the "controller of the file" only referred to person or body "ultimately responsible" for the file and not to "*persons who carry out the operations according to the instructions given by the controller of the file*".[848]

401. COMPARISON WITH THE "DATA CONTROLLER" – While the respective definitions of the terms "controller of the file" and "data controller" bear a close resemblance, they are not identical. In particular, the terms used to describe the object of a controller's decision-making power are slightly different. Under the OECD Guidelines, the data controller decides about the "*contents and use*" of personal data.[849] Under Convention 108, the controller of the file decides about the "*purposes*" of the file, the "*categories of personal data*" that will be stored, and which "*operations*" should be applied to the data. A second difference concerns the absence of language suggesting that the controller is also the "beneficiary" of the file. Neither the text of Convention 108 nor its Explanatory Report contained any language to suggest that the controller of the file was also the party "for whose benefit" the processing of personal data was being carried out.[850] Nevertheless, it seems reasonable to argue that the terms "controller of the file" and "data controller" (as contained the OECD Guidelines) essentially intended to refer to the same type of entity.[851] Moreover, as noted by Bing, even though Convention 108 did not contain an explicit provision regarding "accountability", it similarly (albeit

---

[847] See Explanatory Report, paragraph 32 ("*The reference to the "national law" takes into account the fact that the various national data protection laws contain precise criteria for determining who is the competent person.*") See also P.H. Patrick, "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines", *l.c.*, p. 410.

[848] Explanatory Report, paragraph 32.

[849] Cf. *supra*; nr. 367.

[850] Compare *supra*; nr. 368.

[851] See also J. Bing, "The Council of Europe Convention and the OECD Guidelines on Data Protection", *l.c.*, p. 282. It is also worth noting that F.W. Hondius, who acted as Head of Division II for the Directorate of Legal Affairs of the Council of Europe, approximated the concept of "controller of the record" (which had figured in an earlier draft of Convention 108), with that of a "beneficial user". See F.W. Hondius, "The Action of the Council of Europe with regard to International Data Protection", in OECD, "Transborder Data Flows and the Protection of Privacy", *o.c.*, p. 260. See also *infra*; nr. 403.

less explicitly) rendered the controller of the file ultimately responsible for compliance with its provisions.[852]

402. FROM "USERS" TO "CONTROLLERS" – Convention 108 represented the first instance in which the term "controller of the file" appeared in an official Council of Europe instrument. Its earlier resolution regarding private sector data banks (Resolution (73)22) had not formally specified to whom its principles applied.[853] However, the Explanatory Report suggested that the "*users*" of such data banks were responsible for them.[854] The Explanatory Report went on to note that the "user" or "owner" of a data bank was not necessary the same entity:

> "*Data banks […] may be organised in different ways. The data processing equipment (hardware) and techniques (software) are usually sold or leased by the manufacturers to data processing centres, which contain the data banks. Sometimes the user of the data banks is also the owner and operator of the centre. In most cases, however, the centre is managed by a separate organisation, which has its own operating staff and provides computer facilities to several organisations with data banks.*"[855]

403. GENESIS OF THE "DATA CONTROLLER" CONCEPT – The term "controller" had not figured in any of the national laws adopted prior to Convention 108. As explained earlier, it appears as if the term "controller of the file" emerged in the course of the discussions surrounding the preparation of Convention 108 and the OECD Guidelines.[856]

404. ALLOCATION OF RISK – Convention 108 did not prescribe specific mechanisms of civil or criminal liability. Article 10 merely obliged Parties to establish "*appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter*". This formulation essentially left each State free to determine the nature of these sanctions (civil, administrative and/or criminal).[857]

---

[852] J. Bing, "The Council of Europe Convention and the OECD Guidelines on Data Protection", *l.c.*, p. 282. See also O. Estadella Yuste, "The relevance of the data protection principles set out in Convention 108 and its additional Protocol", report for the *European Conference on Data Protection on "Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: Present and Future" (Warsaw, Poland, 19-20 November 2001)*, p. 57.
[853] See also F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 101.
[854] Explanatory Report accompanying Resolution (73)22, paragraph 15.
[855] *Id.*
[856] Cf. *supra*; paragraph 370.
[857] Explanatory Report, paragraph 60.

3.5 CONCLUSION

405. STRONG SIMILARITY – The provisions of Convention 108 are in many respects similar to those contained in the OECD Privacy Guidelines. Their mutual resemblance comes as no surprise, seeing as many of the delegations to the OECD and Council of Europe meetings were composed of the same experts.[858] Perhaps the most important differences concern the nature of each instrument (a legally binding convention vs. a non-binding recommendation) as well as the geographic constituency of the forum which adopted it (the membership of the OECD notably including countries such as the United States, Canada and Japan).

406. ALLOCATION OF RESPONSIBILITY AND RISK – As we have seen, a strong similarity also exists with regards to how both instruments allocate responsibility and risk. Both instruments designated the "controller" as the actor that should be "ultimately responsible". Convention 108 referred to the "controller of the file" whereas the OECD Guidelines referred to the "data controller". Notwithstanding subtle differences in their respective definitions, both terms seemingly intended to refer to the same type of actor. Conspicuously absent from Convention 108 and its Explanatory Report, however, is a reference to any obligations of entities which might be acting "on behalf" of the controller. Contrary to the OECD Guidelines, there is no mention in Convention 108 of the Parties' ability to introduce "more complex schemes of levels and types of responsibilities" (e.g., by imposing certain obligations on so-called "service bureaux" or "data processing centres").[859] However, given the close relationship between the two texts, one must remain cautious not to overstate the significance of this omission.

407. AFTERMATH – As the preparation of Convention 108 drew to an end, the Council of Europe began directing its efforts in the area of data protection towards specific sectors of activity. The first sector of activity to be studied was the medical sector, which resulted in Recommendation R(81)1 on Regulations for automated medical data banks.[860] It then went on to develop recommendations regarding the use of personal data for scientific research and statistics[861], for the purposes of direct marketing[862], for

---

[858] J. Bing, "The Council of Europe Convention and the OECD Guidelines on Data Protection", *l.c.*, p. 285; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 130-140 H. Burkert, "Privacy - Data Protection A German/European Perspective", *l.c.*, p. 52.

[859] Compare *supra*; nr. 371.

[860] Committee of Ministers of the Council of Europe, "Recommendation R(81)1 on Regulations for automated medical data banks", 23 January 1981 (328th meeting of the Ministers' Deputies).

[861] Committee of Ministers of the Council of Europe, "Recommendation R(83)10 on the protection of personal data used for scientific research and statistics", 23 September 1983, (362nd meeting of the Ministers' Deputies).

[862] Committee of Ministers of the Council of Europe, "Recommendation R(85)20 on the protection of personal data used for the purposes of direct marketing", 25 October 1985, (389th meeting of the Ministers' Deputies).

social security purposes[863], etc. A formal review process of Convention 108 was launched in 2010, which is currently still ongoing.[864]

[863] Committee of Ministers of the Council of Europe, "Recommendation R(86)1 on the protection of personal data for social security purposes", 23 January 1986, (392nd meeting of the Ministers' Deputies). Each of the aforementioned Resolutions can be downloaded at http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (last accessed 8 November 2013).

[864] This review process is commonly referred to as the "modernization of Convention 108". For more information see http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

Chapter 5 NATIONAL DATA PROTECTION LAWS AFTER 1981

408. OUTLINE – This chapter will analyse two data protection laws enacted after 1981, namely the UK Data Protection Act of 1984 and the Belgian Data Protection Act of 1992. The objective of this analysis is to track the further development of EU data protection laws leading up to Directive 95/46. In the interest of brevity, the discussion of each act shall be reduced in scope. The discussion will be limited to (1) the origin and development of the act (in order to place it in context) and (2) the allocation of responsibility and risk. Substantive rights and obligations are not discussed separately, as these provisions correspond, by and large, to the provisions of Convention 108 and the OECD Privacy Guidelines.

1 UNITED KINGDOM (1984)

1.1 ORIGIN AND DEVELOPMENT

409. EARLY INITIATIVES – The UK Data Protection Act of 1984 had been a long time coming. The first legislative proposals concerning privacy emerged in the early 1960s, under the form of private member bills. These bills mainly sought to introduce a general right to privacy.[865] At the time, there was a growing sentiment that traditional remedies (e.g., the law of torts or breach of confidence) did not offer sufficient protection against intrusions facilitated by modern technologies.[866] None of these proposals made much of an impact, however, until the *Right to Privacy* bill of 1969.[867] This bill was closely connected to a controversial Justice report entitled "*Privacy and the Law*" (1970).[868] While the Right to Privacy bill was not adopted, the ensuing debate did induce the

[865] See Home Office (Great Brittain), *Report of the Committee on Data Protection*, Cmnd. 7341, HMSO, London, 1978, p. 3; F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 49 and J. A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives*, *o.c.*, p. 40-41.

[866] F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 49. See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 83.

[867] Right to Privacy Bill, *HC Deb* 26 November 1969, vol. 792, c. 430. Appendix F of the report of the Younger Committee contains a copy of this bill as well other privacy-related bills. (See Home Office (Great Brittain), *Report of the Committee on Privacy*, Cmnd. 5012, HMSO, London, 1972, p. 273 et seq.) A summary of the discussions surrounding the proposals can be found at p. 185-202.

[868] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 1; F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 49 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 107. The Justice report was met with hostility from the UK press, who felt that a general right to privacy might restrict their freedom of speech. See G. Dworkin, "The Younger Committee Report on Privacy", *The Modern Law Review* 1973, Vol. 36, No. 4, p. 399 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 84-85.

Government to appoint a Committee on Privacy, better known as the "Younger Committee".[869]

410. YOUNGER COMMITTEE – The Younger Committee was tasked to investigate whether legislation was necessary "*to give further protection [...] against intrusions into privacy by private persons and organisations, or by companies*".[870] Its mandate of inquiry was thus confined to the private sector. [871] In 1972, the Committee found that it would be unwise to create a general right to privacy.[872] It also felt that the introduction of data protection legislation would be premature as the use of computers did not yet form a threat to privacy.[873] It did, however, recommend that computer users voluntarily adopt certain principles for handling personal information on computers.[874] It also recommended that the Government "*provide itself with machinery, such as a standing commission, for keeping under review the growth and techniques of gathering personal information on computers*".[875]

411. GOVERNMENT WHITE PAPER – After some years of delay, the UK Government issued a White Paper entitled "*Computers and Privacy*" (1975).[876] The White Paper outlined the position of the Government following the Younger Report as well as the Government's inquiry into its own use of computer systems. Somewhat surprisingly, the White Paper announced that there was a need for data protection legislation after all.[877] While maintaining that fears about improper use of computers were still unjustified, the Government considered that legislation for both the public and private sector was

---

[869] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 1. See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 107 and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 85.

[870] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 1.

[871] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 2. See also G. Dworkin, "The Younger Committee Report on Privacy", *l.c.*, p. 399. The Younger Committee analysed many different aspects of the "privacy problem" (the concept, areas of concern, practices in specific sectors) as well as technological developments relating to surveillance devices and computers.

[872] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 202 et seq. See also G. Dworkin, "The Younger Committee Report on Privacy", *l.c.*, p. 401 and F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 50.

[873] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 191.

[874] Id. See also p. 183-185. These principles, which had been developed by British Computer Society, proved quite influential and informed not only the later development of the UK Data Protection Act, but also the development of data protection laws around Europe. (F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 52 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 107.)

[875] Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 191. For a general evaluation of all the recommendations proposed by the Younger Committee see G. Dworkin, "The Younger Committee Report on Privacy", *l.c.,* p. 401 and F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 400-406.

[876] Home Office (Great Brittain), *Computers and Privacy*, Cmnd. 653, Her Majesty's Stationary Office (HMSO), London, 1975; reproduced by Home Office (Great Brittain), *Report on the Committee on Data Protection*, *o.c.*, p. 449-460.

[877] Commentators have ascribed this change of heart to the fact that UK data processing companies were losing business because of restrictions imposed by data protection legislation in other countries. See e.g. J. A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives*, *o.c.*, p. 41.

necessary in order to prevent misuse in the future.[878] The White Paper went on to describe what this legislation should look like, leaving further details to be defined by yet another committee.[879]

412. THE LINDOP COMMITTEE – The Committee on Data Protection, chaired by Sir Norman Lindop, presented its findings in December 1978. The Committee recommended the establishment of an independent body (the "Data Protection Authority" or "DPA"), whose duty it would be to supervise compliance with a set of statutory principles defined in the future data protection act.[880] These data protection principles would not be directly enforceable in courts.[881] Rather, the principles would serve as the basis for future *Codes of Practice* which would govern different types of personal data handling activities.[882] One of the main tasks of the Data Protection Authority was to draw up such Codes of Practice in consultation with the affected users.[883]

413. LEGISLATIVE DEVELOPMENT – It was not until 1982 that the UK Government published a new White Paper confirming its intent to legislate.[884] On 21 December 1982, the Government presented a draft data protection bill in Parliament.[885] This bill differed from the recommendations offered by the Lindop Committee in several respects.[886] Most notably, the previously recommended "Data Protection Authority" had been reduced to a mere "Data Protection *Registrar*", whose powers were more limited in scope.[887] According to commentators, the main objective of the 1982 bill was simply to enable the UK to ratify Convention 108, which the UK had already signed in 1981.[888] The bill was

---

[878] Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 6.
[879] *Id*.
[880] Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 163; A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 108.
[881] Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 163.
[882] *Ibid*, p. 164. The main objective of this approach was to ensure sufficient flexibility, given wide range of contexts in which personal data are used. See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 108 and A. Crook, "Data Protection in the United Kingdom, Part 2", *Journal of Information Science* 1983, Vol. 7, p. 48.
[883] Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 164.
[884] Home Office (Great Brittain), *Data Protection: the Government's proposal for Legislation*, Cmnd. 8539, HMSO, London, 1982, 23 p. The second push towards the enactment of legislation has likewise been attributed to the UK computer industry: see e.g., J. McBride, "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)", *Les Cahiers de Droit* 1984, vol. 25, n° 3, p. 535; A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 108and C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 90-91.
[885] House of Lords (HL) Debates (Deb), 21 December 1982, vol. 437 c. 926 (accessible at http://hansard.millbanksystems.com/lords/1982/dec/21/data-protection-bill-hl).
[886] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 109.
[887] *Id.*
[888] One member of the House of Lords commentator later characterized the bill as trying to do nothing more than achieve "bare compliance with the terms of the European Convention" See HL Deb 20 January 1983 vol. 437 cc 1551 (accessible at http://hansard.millbanksystems.com/lords/1983/jan/20/data-protection-bill-hl-1). See also C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 93.

reintroduced on 23 June of 1983.[889] After a series of legislative amendments, the UK Data Protection Act was finally signed into law on 12 July 1984.[890]

1.2 ALLOCATION OF RESPONSIBILITY AND RISK

414. OUTLINE – The long legislative history of the UK Data Protection Act left behind a rich body of literature. The following sections will analyse how the views of UK policymakers evolved over time with regard to the allocation of responsibility and risk. Specifically, an analysis shall be made of the views of (A) the Younger Committee (1972); (B) the Lindop Committee (1978); and (C) the drafters of the UK Data Protection act (1984).

A. The Younger Committee

415. PROFESSIONAL DISCIPLINE – As mentioned earlier, the Younger Committee had decided that the time for data protection legislation was not yet ripe.[891] However, the Committee did propose a set of principles for the handling of personal information by computers.[892] These principles were to be observed, on a voluntary basis, by "*computer manufacturers, operators and users*".[893] The Younger Committee further envisaged a system of control through professional discipline, whereby one or more professional associations would impose a set of ethical standards upon those "*responsible for programming and operating computers*".[894]

416. CONCEPT OF A "RESPONSIBLE PERSON" – The Younger Committee also recommended to consider whether it might be useful if each organisation handling computerized personal information were to appoint a "responsible person" within its organisation.[895] Such a responsible person would be

---

[889] J. McBride, "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)", *l.c.*, p. 533. The bill needed to be introduced a second time due to the dissolution of Parliament for the general election. (*Id.*)

[890] Data Protection Act, 1984 c. 35. A copy scanned copy of the original 1984 UK Data Protection Act is accessible at http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf (last accessed 3 September 2014). For a summary overview of the Parliamentary debates see A. Crook, "Data Protection in the United Kingdom, Part 2", *Journal of Information Science* 1983, Vol. 7, p. 47-57.

[891] Cf. *supra*; nr. 410.

[892] See Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 182 et seq.

[893] *Ibid*, p. 184.

[894] *Ibid*, p. 185. However, the Committee concluded that it was "*premature to expect the successful establishment in the near future of an effective voluntary professional discipline which could properly be endorsed by legislation*". (*Id.*)

[895] *Ibid*, p. 16 and p. 191.

> "*the person to whom the owner or user of a computerized personal information store has delegated the responsibility for ensuring that whatever principles the legislation requires him to enforce are complied with […]*".[896]

While the final responsibility for compliance would remain with the "owner" or "user" of the data processing system, the responsibility for the enforcement within the organisation would be delegated to this responsible person.[897]

417. USERS VS. COMPUTER BUREAUX – The Younger Committee recognized that not every user of a computer system owned the underlying equipment. Specifically, it recognized the existence of so-called "computer bureaux", who provided computing services on an agency basis.[898] The Younger Committee considered that

> "*[i]n the case of a commercial computing bureau, only some of the requirements contained in the principles would fall within the competence of the bureau operator/owner, the remainder being the responsibility of the user. Nevertheless it would probably be necessary that bureaux also should appoint "responsible persons", as to secure to the maximum degree the enforcement of those requirements which are within their competence."*[899]

418. DISTRIBUTION OF RESPONSIBILITY – When discussing the division of responsibility between the users and providers of computing services, the Younger Committee made a distinction between three areas, namely:

> "*i. The computer services area, which includes the translation of the designed system into programs of instruction to the machine installation, the operation of the installation together with its input and output facilities and the monitoring of the installation's performance and of the required security provisions.*
>
> *ii. An area where there is joint involvement between the user and the person or persons who provide the computer services. This area will include, inter alia, the design of systems to meet the user's requirements, the checking of such systems to ensure that the requirements have been met, the nature and extent of security provisions to be incorporated into the systems and the safeguarding of information in transit between the user and the computer service whether by document, telephone, teleprinter or terminal.*

---

[896] *Ibid*, p. 336. The Younger Committee compared the function of the "responsible person" to that of a "Security Administration Officer" who is tasked with ensuring the efficient operation and audit of measures prescribed for data security. (*Id.*)

[897] *Id.* Again, the Younger Committee felt that further study was necessary before introducing a legal requirement mandating the appointment of a "responsible person". (*Ibid*, p. 192)

[898] *Ibid*, p. 192. The role of computer bureaux was studied at length by the Lindop Committee. Cf. *infra*; nrs. 421 et seq.

[899] *Ibid*, p. 336.

> *iii. The area where responsibility must lie with the ultimate user of the service who will initiate and specify the requirements to be met, will probably be responsible for routine assembly of the information for input to the computer and who will use the processed information when it is supplied to him from the computer. […]"*[900]

The Younger Committee thus clearly foresaw responsibilities for both users and bureaux, each within their own sphere of competence.

B. The Lindop Committee

419. TERMINOLOGY – The Lindop Committee had been tasked to provide recommendations for the enactment of data protection legislation.[901] With this task in mind, the Committee set out to find appropriate terminology to identify the subjects of the future data protection act.[902] After discarding several alternatives (such as "operator" and "owner"), the Committee eventually settled on the term "user" to denote the main subject of regulation.[903] The Committee selected this term because it was generally used in computing circles to refer to "*those who use computers for their own purposes – as opposed to those who provide others with a computer service for a fee*".[904] The latter were referred to as "data handling bureaux" or "computer bureaux". While bureaux would not be subject to the same obligations as users, they would nevertheless become subjects of the Lindop Committee's recommendations.

420. DEFINITION OF A "USER"– In its "principal legislative recommendations", the Lindop Committee defined a "user" as:

> "*any person who, alone or with others, carries on or causes to be carried on any automatic handling of personal data in any part of the UK wholly or partly for his own interest, and determines what data are handled.*"[905]

The Committee likened the concept of a user to that of the "beneficial user", which had previously been defined by the Computing Services Association (CSA) as

> "*the organisation or individual who uses personal data in his business or other activities and who is entitled to give instructions for a personal record data system to be designed and programmed (including subsequent amendments), processed or operated*".[906]

---

[900] *Ibid*, p. 337 (emphasis added).
[901] Cf. *supra*; nr. 412.
[902] Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 149-150.
[903] *Ibid*, p. 150.
[904] *Id.*
[905] *Ibid*, p. 289.
[906] *Ibid*, p. 150.

421. DEFINITION OF A "BUREAU" – Although the Lindop Committee did not propose a definition for the term "bureau", it had studied the phenomenon of bureaux in detail.[907] The Committee described a data handling bureau as an organisation which made its (computing) facilities available to others for the purpose of executing their data handling applications.[908] The services offered by a bureau could vary widely, ranging

> *"from just the hire of computer time for use by the user's own staff to the full range of* ad hoc *systems design, programming, data preparation, computer output handling to meet individual user needs, and the provision of standardised and packaged comprehensive information services which are sold in identical form to many clients. […] Statistical aggregations or customer billing or payroll are the sorts of tasks which are commonly taken on from day to day."*[909]

422. DISTINGUISHING "USERS" FROM "BUREAUX" – According to the Lindop Committee, there were two attributes distinguishing users from bureaux. First, a user handles data (or has them handled) for his own interest, and not as an agent for someone else.[910] Second, a user also determines what data are to be handled.[911] These two characteristics set users and bureaux apart from one another.

423. RELATIONSHIP BETWEEN USERS AND BUREAUX – The bureau was seen by the Lindop Committee as an agent of the user, who acted under the latter's instructions.[912] Usually, the specific responsibilities of the bureaux would be set out in a contract between the user and the bureau.[913] While the bureau's services might be constrained by its resources (e.g., available equipment), it would in principle not be selective in what it did.[914] It was the user (and not the bureau) who decided what services would be provided and how the data would be used.[915] However, in many cases the customer would also rely heavily on the bureau for technical advice on how the work should be handled.[916] Furthermore, it was not uncommon for all stages of a job, from data collection to dissemination, to be handled on an agency basis.[917]

---

[907] *Ibid*, p. 252-259.
[908] *Ibid*, p. 252.
[909] *Ibid*, p. 255. It is worth noting that a bureau was not necessarily aware of the fact that it was handling personal data (or why). In some cases a bureau might have had knowledge and understanding of the data it handles (and of the meaning of the products which result from that handling), in other cases it might not. For example, if the bureau's facilities were operated by the user's own staff (something which was frequently done by terminal access), the bureau staff might not have been aware of what programs were used or of the processes that were undertaken. (*Id.*)
[910] *Ibid*, p. 150.
[911] *Id.*
[912] *Ibid*, p. 255-256.
[913] *Id.*
[914] *Id.*
[915] *Id.*
[916] *Id.*
[917] *Ibid*, p. 256. Despite the potential latitude of a bureau's role, the Lindop Committee considered that "*it is the final user of the information who decides what will be done once the bureau has produced what is wanted.*" (*Ibid*, p. 255.)

424. BUREAUX AS SUBJECTS OF REGULATION – For the Lindop Committee, it was clear that the decision-making power of bureaux was much more limited in comparison to that of users.[918] At the same time, it also recognized that certain aspects of data protection did reside within the competence of a bureau. For example,

> "*[t]he maintenance of the accuracy of the data during handling [...] and the maintenance of an adequate standard of security, are matters which depend on the efficiency and reliability of staff and equipment, the design of software and the physical safeguards at the location of data handling*".[919]

The Lindop Committee felt that bureaux should be made directly responsible "*for complying with data protection rules in those matters over which they had control*".[920] It explicitly rejected the approach advocated by the CSA, according which only users would be directly responsible for compliance.[921] It motivated this conclusion by reasoning that

> *"Users are generally not in a position to assess the reliability or competence of bureau, no matter how strong the incentive on them to do so may be. Consequently, compliance with data protection rules where applications are handled by bureaux would not be effectively supervised."*[922]

Moreover, the Committee reasoned, some users might be deterred from taking full advantage of the benefits of automation if they risked being penalized for breaches caused by a bureau without being able to recover damages.[923]

425. ALLOCATION OF RESPONSIBILITY – According to the Lindop Committee, each party subject to the act should be responsible for those aspects over which they have control. The exact distribution of responsibility would not, however, be specified in the act itself. Instead, the Data Protection Authority would have the task of defining the appropriate division of responsibilities in *Codes of practice*.[924] It was already clear from the beginning, however, that users would be subject to the bulk of the act's obligations:

---

[918] *Ibid*, p. 256.

[919] *Id*. The Committee considered moreover that "*the user-bureau relationship brings with it certain additional potential hazards to data protection, which are note present where the data are handled by the user's own staff and on his own facilities. One such risk arises from the fact that the user's application may run side by side with the applications of other users employing the same bureau: in some circumstances this could give rise to possibilities for accidently allowing one user access to another's data [...].*" (*Id.*)

[920] *Ibid*, p. 257 and 295.

[921] *Ibid*, p. 256-257. Under this approach, users might be required to exercise reasonable care when entrusting their data handling to a third party. In their contracts with bureau, users could require indemnities in case of any breach of a Code of Practice caused by the bureau. In this way, "*[l]iability for matters within its competence would pass to the bureau indirectly through the civil law, since it would be required to compensate the user for any penalties or civil damages incurred by him [...]*." (*Ibid*, p. 257.)

[922] *Ibid*, p. 257.

[923] *Id*.

[924] *Ibid*, p. 258. As mentioned earlier, the Lindop Committee recommended that future data protection act should contain "a set of statutory principles" (e.g., data accuracy, purpose specification). These data protection principles would not be directly enforceable in courts. Rather, the principles would serve as the basis for future Codes of Practice, which would govern different types of personal data handling

> *"In the relationship between user and bureau, it is the user who retains control over the nature of the data being handled, the methods by which it is collected, the degree of access which he accords to his data subjects, and the purposes to which the data are put. […] [T]he bureau often has no effective means of controlling these aspects […] We agree therefore with the CSA that there can be no question of placing legal responsibility for complying with these matters on any person other than the user."*[925]

The obligations incumbent upon bureaux would mainly concern security measures for safeguarding the confidentiality and integrity of data.[926] Nevertheless, each Code of Practice would specify in it "*those provisions which become binding on any bureau which handle applications in the relevant category*".[927] Breach of those provisions would be an offence, and

> "*it would therefore be incumbent on a bureau to avoid taking on an application if it was unable to meet the safeguards and standards required for that application under the relevant code*".[928]

The Lindop Committee also considered that the Data Protection Authority may wish to draft one or more Codes of Practice which would be applicable to bureaux "as a class".[929] Finally, it is worth noting that the Committee even foresaw an advisory role for bureaux, especially towards small users who may not be aware of the contents of the relevant Codes of Practice.[930]

426. ALLOCATION OF RISK – Both users and bureau would be liable in case of a violation of a relevant Code of Practice. However, each party would only be liable for its own offences and for matters within its control.[931] As a result, the overall liability exposure of bureaux was considered to be more limited as their sphere of competence primarily concerned security measures.[932] Nevertheless, it would be an independent offence for a bureau to fail to comply with provisions of codes of practice which reside with the bureau's competence.[933] Finally, it is also worth observing that the Data Protection Authority would have similar powers of supervision over bureaux as it would

---

activities. It was expected that the Data Protection Authority would define, for each class of personal data handling applications, which measures users should be taken. Cf. *supra*; nr. 412.

[925] *Ibid,* p. 256 (emphasis added).

[926] *Ibid*, p. 258.

[927] *Id*.

[928] *Id*.

[929] *Id*. Such codes might deal with "*such matters as the need to avoid any linking of the different applications of different users, and the need to avoid any accidental or deliberate retention of data when the bureau ceased to carry out work for a user.*" (*Id*.)

[930] *Ibid*, p. 259.

[931] The Lindop Committee explicitly rejected the notion of vicarious liability, at least insofar as criminal liability was concerned. It considered that it would be "*distasteful to impose on users absolute criminal liability of the transgression of others who were beyond their control*". (*Ibid*, p. 257).

[932] *Ibid*, p. 258.

[933] *Id.*

over users, meaning that bureaux could be held accountable in a manner similar to users.[934]

C. The 1984 Data Protection Act

427. TERMINOLOGY – The 1984 Data Protection Act retained, by and large, the terminology developed by the Lindop Committee. The Act employed the term "data user" to denote the main subject of regulation. It also followed the Committee's recommendation to bring "computer bureaux" within the scope of the act. The definition of each term, however, was extended in order to align it with the other terms defined in the act.

i. Data user

428. DATA USER – Section 1(5) of the 1984 Data Protection Act defined a data user as

"*a person who holds data, and a person 'holds' data if –*

(a) the data form part of a collection of data processed or intended to be processed by or on behalf of that person […]; and

(b) that person (either alone or jointly or in common with other persons) controls the contents and use of the data comprised in the collection ; and

(c) the data are in the form in which they have been or are intended to be processed […]."[935]

429. "A PERSON" – In principle, every natural or legal person could be characterized as a data user.[936] The term encompassed both individuals as well as bodies of persons, such as corporate bodies, unincorporated bodies, trade unions, governmental departments[937], trade associations, etc.[938] The concept was not confined to commercially operating entities.[939] However, individuals holding personal data "*which concerned only*

---

[934] *Id.*

[935] Emphasis added. The term "data" was defined by Section 1(2) as "*information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose*".

[936] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 111.

[937] See HL Deb, 24 March 1983, vol. 440, at cc 1275-1276 for a discussion of the possibility that government departments be qualified as data users (accessible at http://hansard.millbanksystems.com/lords/1983/mar/24/data-protection-bill-hl#S5LV0440P0_19830324_HOL_110)

[938] C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 81. Employees or individuals acting on behalf of an organisation were generally considered as data users themselves (in such case the data user was the employer or organisation for whom they worked). See The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", Office of The Data Protection Registrar, Cheshire, 1985, p. 2 (Question 3); The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Guideline: number 2, Office of the Data Protection Registrar, Cheshire, 1989, p. 26-27

[939] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 111.

the management of his personal, family or household affairs or held by him for recreational purposes" were exempted from compliance with the DPA (section 33(1)).[940]

430. "CONTROLS THE CONTENT AND USE" – Not every person processing personal data was considered a data user.[941] A person was only considered a data user if this person actually "held" the data within the meaning of Section 1(5).[942] "Holding" in this context did not mean "possession".[943] A person was considered to "hold" data only if that person *controlled its contents and use*.[944] The term "control" was thus at the heart of the definition of a data user. [945] In 1985, the term was further clarified by Data Protection Registrar as follows:

> "*Controls – this is a vital element of the definition. You are not a "Data User" and do not "hold" data unless you are entitled to take the final decision as to the information which is to be recorded and as to the purposes for which the data are to be used*."[946]

---

[940] See also HL Deb 10 March 1983 vol. 440, at cc373, for a discussion of the rationale behind the "personal use" exemption (accessible at http://hansard.millbanksystems.com/lords/1983/mar/10/data-protection-bill-hl. Strictly speaking, data held for private purposes was only partially exempted from the 1984 Data protection act (see section 33(1). In principle, the users of these data still needed to comply with the general principles of data protection contained in Section 1 of the act. However, in practice there was a total exemption as the principles were only enforceable against registered data users. A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 118 footnote 21. The 1984 Data Protection Act provided similar blanket exemptions for personal data (1) which the law requires to be made public; (2) which safeguard national security; (3) held for payroll, pensions and accounts purposes; (4) from unincorporated member clubs and (5) in mailinglists. In addition, the DPA also contained exemptions from certain obligations in certain situations (e.g. exemption to non-disclosure obligation in case the disclosure is required by law). See A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 118-119.

[941] The Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", Guideline: number 1, Office of the Data Protection Registrar, Cheshire, 1984, p. 12.; A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 111.

[942] The Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", *l.c.*, p. 12.

[943] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Guideline: number 2, Office of the Data Protection Registrar, Cheshire, 1989, p. 9.

[944] As noted by Lord Elton: "*The key concept here is the control of the contents and use of data. That is the crucial element in the definition of data user because it is only the person who controls contents and use who can sensibly be expected to fulfil the responsibilities and obligations that the Bill places on data users.*" HL Deb, 19 July 1983, vol. 443, cc1068 (accessible at http://hansard.millbanksystems.com/lords/1983/jul/19/data-protection-bill-hl#S5LV0443P0_19830719_HOL_67. Effective control over how the data was to be used was considered to be especially important. See also HL Deb 10 March 1983 vol. 440, at cc. 408-409, accessible at http://hansard.millbanksystems.com/lords/1983/mar/10/data-protection-bill-hl#S5LV0440P0_19830310_HOL_111 (stating that "the person to be held responsible under the Bill is the person who actually controls what is to be done with the data").

[945] See HL Deb 19 July 1983 vol. 443, at cc 1069, accessible at http://hansard.millbanksystems.com/lords/1983/jul/19/data-protection-bill-hl#S5LV0443P0_19830719_HOL_67.

[946] The Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", *l.c.*, p. 12 (emphasis added).

A person was said to control the "*contents*" of a data collection if he is "*in a position to decide which item and type of information are to be recorded as data*".[947] A person controls the "use" of the collection if he is "*able to determine the purpose for which the data are to be processed*".[948]

In 1989, the Data Protection Registrar further expanded on the notion of "control" as follows:

> "*Control means having the power to decide what information about an individual is to be recorded, whether the information should be added to, amended or deleted and to what use the recorded information may be put either by the data user or by others. This is not the same as physically controlling either the processing operations or the disk or tapes on which the data are recorded.*"[949]

431. "DATA PROCESSED OR INTENDED TO BE PROCESSED" – Mere collection or storage of data without any intention to see these data processed automatically fell outside the scope of the DPA.[950]

432. "BY OR ON BEHALF OF" – It was not necessary to possess a computerized system in order to be considered a data user.[951] A company which made use of the services of a computer bureau would also be considered as a data user within the meaning of the DPA, provided that it exercised control over the contents and use of automated personal data.[952]

433. "ALONE OR JOINTLY OR IN COMMON" – The drafters of the 1984 Data Protection Act recognized that control could be exercised by more than one entity.[953] As stated by the Data Protection Registrar:

> "*The control does not need to be exclusive to one data user. Control may be shared with others. It may be shared jointly or in common. 'Jointly' covers the situation where control is exercised by acting together. Control 'in common" is where each*

---

[947] The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", *l.c.*, p. 1.
[948] *Id.*
[949] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 10.
[950] *Id.* and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 111. See also HL Deb, 19 July 1983, vol. 443, at cc 1054-1055 (discussing a proposed amendment to add the word "collecting" to the definition of data user) and cc 1067-1068 (discussing the relevance of the intention to process). Processing" was defined by Section 1(7) as "*amending, augmenting, deleting or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operation by reference to the data subject*".
[951] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 112.
[952] *Id.*
[953] See HL Deb 19 July 1983 vol. 443, at cc 1069 (discussing a scenario of "joint control"), accessible at http://hansard.millbanksystems.com/lords/1983/jul/19/data-protection-bill-hl#S5LV0443P0_19830719_HOL_67.

shares a pool of information, changing, adding to or using the information for his own purposes independently of the other".[954]

ii. Computer bureau

434. COMPUTER BUREAU – According to Section 1(6) of the 1984 Data Protection Act, a person carries on a computer bureau if

> "*he provides other persons with services in respect of data, and a person provides such services –*
>
> *(a) as agent for other persons he causes data held by them to be processed […]; or*
>
> *(b) he allows other persons the use of equipment in his possession for the processing […] of data held by them.*"[955]

435. "A PERSON" – In principle, both natural and legal persons could act as a computer bureau.[956] A person did not have to be in business as a bureau in order to meet the definition of a computer bureau.[957] Nor was it necessary that the person takes part in the actual processing of the data. It was sufficient that he made equipment in his possession available for use by a data user.[958]

436. "SERVICES IN RESPECT OF DATA" – The 1984 Data Protection Act distinguished between two types of services offered by a computer bureau, namely (a) the processing of personal data held by others and (b) the making available of equipment to process data held by others. This definition reportedly covered a variety of arrangements

> "*from the traditional batch bureau offering […], such as batch accounting or payroll functions, to those where the user, inputting his own materials, has direct access to mainframe processing capabilities […]*".[959]

---

[954] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", l.c., p. 10-11. See also the Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", *l.c.*, p. 12 (*""jointly or in common" - covers the situation where control is exercised by a number of persons acting together or by each of a group of persons."*). It is interesting to note that while the definition of a data user provided by the Lindop committee recognized that control might be exercised together with others (i.e. "jointly"), it did not explicitly recognize that multiple entities might be controlling data at the same time, but each for their own purposes (compare *supra*; nr. 421).

[955] Emphasis added.

[956] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 112 and C. Edwards and N. Savage, "Data Privacy: the UK Experience", in C. Edwards and N. Savage (eds), *Information Technology & The* Law, 1986, MacMillan Publishers, p. 81.

[957] The Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", *l.c.*, p. 12.

[958] *Id.*

[959] T. Cook, "The law relating to computer bureaux", in C. Edwards and N. Savage (eds), *Information Technology & The* Law, 1986, MacMillan Publishers, p. 159. The author further notes that for many computer bureau their computer activities might be but a small part of the overall service which they offer. For example, a traditional batch bureau payroll service could be combined with the secure delivery

437. "AS AGENT" – The definition of a computer bureau implied that any processing of personal data by the bureau occurred on an agency basis. According to the Data Protection Registrar, however, "agency" in this context merely meant "*a person acting for others*" rather than as an agent in a contractual sense.[960] Because a computer bureau acted "on behalf" of a data user, it was in principle not allowed to disclose personal data without prior authorization by the data user who controls that data (section 15(1)).[961]

438. "ALLOWING THE USE OF EQUIPMENT" – Paragraph (b) of the definition covered the situation where a person allowed others to make use of computer equipment in his possession, without taking active part in the processing.[962] The term "possession" did not refer to ownership but merely implied physical control of the equipment.[963]

iii. Distinguishing "users" from "bureaux"

439. KEY CHARACTERISTICS – Similar to the definitions provided by to the Lindop Committee, there appear to be two key characteristics distinguishing data users from computer bureaux. First, a data user processes data (or has them processed) for his own purpose(s), and not as an agent for someone else. Second, the data user also decides what data (contents) are to be handled.[964]

440. SCENARIOS – Already in 1985, the Data Protection Registrar observed there might be scenarios in which it could be difficult to distinguish between "data users" and "computer bureaux":

> "*Difficulties in identifying the Data User may arise where one organisation (A) has services provided to it by another organisation (B) and, in order to provide those services, B automatically processes personal information supplied by A.*"[965]

By way of illustration, the Registrar described 3 scenarios to clarify the distinction between data users and computer bureaux in such cases:

> *ii) "Where A instructs or requests B to process the information on A's behalf, the nature of the output and the purposes of which it is to be used is being determined by A, then B is merely carrying out the processing on behalf of A. If*

---

of wages, or a remote access bureau could be combined with the writing of customized programs to the requirements of the user. (*Ibid*, p. 160.)

[960] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 12.

[961] See also HL Deb, 21 July 1983, vol. 443, at cc 1299-1300, accessible at http://hansard.millbanksystems.com/lords/1983/jul/21/data-protection-bill-hl#S5LV0443P0_19830721_HOL_155 (discussing the exemption to the non-disclosure requirement for access requests by law enforcement and its relationship to computer bureaux).

[962] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 12.

[963] *Id.*

[964] Compare *supra*; nr. 422.

[965] The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", *l.c.*, p. 2 (Question 2).

this is done automatically than A is a Data User and B is a Computer Bureau. […][966]"

iii) "*Where the automatic processing of the information is merely incidental to some other service which B provides to A, the decisions as to the information to be processed and the purpose of processing being made by B on his own account, the B is the data user. […][967]"*

iv) *"If B is both processing on behalf of A and providing some other service then both A and B may be Data Users […] In respect of this information A and B control the contents and use of the data in common and both are Data Users. […]"*[968]

The Registrar also described the scenario in which the service provider does not receive the data from the client, but rather is in a situation where he collects information and maintains records which he decides are necessary to provide the service. The example provided is that of an estate agent, who manages residential properties on behalf of its owner. Because the estate agent had been given a "wide discretion" by the property owner as to the actual contents and use of the records, the estate agent was considered to be the data user rather than the owner (because the owner's interest was essentially only in the income received rather than in the contents of the individual records).[969]

441. ROLE OF CONTRACTS – The UK Data Protection Act did not formally require the creation of contract among data users and computer bureaux. Where such contracts existed, however, its terms could be relied on by the Registrar to determine whether a party was acting either as data user or as a computer bureaux.[970] The Registrar immediately added, however, that a contract to decide which of the parties is the data user "*must not be a sham*".[971] According to the Registrar, the contract should leave the data user free to make at least some of the following decisions:

- *"to what extent records containing information about individuals should be kept;*

---

[966] The example provided by the Registrar is that of an accounting firm, whereby B both keeps the accounts of A's business and calculates the salaries of its employees.
[967] The example provided by the Registrar is that of a tax consultancy firm, whereby B processes the information provided by A in order to provide advice on the A's tax affairs.
[968] In the example provided by the Registrar B both keeps the accounts A and provides tax advice to A. (The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", *l.c.*, p. 2 (Question 2)).
[969] The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (21-34)", Office of The Data Protection Registrar, Cheshire, 1986, p. 3-4 (Question 22). See also The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 29-31 (providing further examples to determine whether the customer or the service provider should be considered the data user).
[970] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 27. ("*If it is clear from the contract that one of the parties accepts all of the responsibilities under the Act and that he is genuinely in a position to fulfil those responsibilities, then there should be no difficulty in concluding that that person is the data user and that the other party is not. It will, therefore, be sensible for those who are in this situation to review their contracts and to consider whether their positions are already clear or whether some more terms should be added to the contract to clarify the situation.*")
[971] *Id.*

- *what sort of information about individuals they should contain;*
- *from where that information should be obtained;*
- *when and how the information should be processed;*
- *whether or not the information is accurate or should be updated;*
- *whether and when the information should be added to, amended or deleted;*
- *whether and when the information should be available to the other party;*
- *whether the information may be disclosed to and used by third parties;*
- *what information should be made available to an individual who makes a subject access request under the Act and whether information should be withheld in reliance on one of the exemptions from the subject access provisions; and*
- *whether the data user may keep the information after the contract has ended."*[972]

iv. Allocation of responsibility and risk

442. OUTLINE – The 1984 Data Protection Act was underpinned by eight data protection principles based on the Younger Committee's Report and Council of Europe Convention 108.[973] Because of their general nature, the principles were not directly enforceable through the courts, but only indirectly through the Registrar.[974] The first seven principles applied only to data users, i.e. those who controlled the content and use of the data held.[975] The eighth principle (security) applied both the data users and computer bureaux (Section 2(2)).[976] Both data users and computer bureaux were under an obligation to register themselves with the Data Protection Registrar (Section 5(2) and 5(4)).[977]

---

[972] *Ibid*, p. 28. Interestingly, the Data Protection Registrar also linked the concept of the data user to the *business interests* of the parties involved. The customer of the service will need to retain its role of data user if he is not able to surrender control over the contents and use of the information without losing control over the running of its own business. (*Ibid*, p. 29) In an earlier text, the Registrar also linked the concept of a data user to the concept of *ownership*, by asking to whom the data resulting from the processing "belong". See The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (21-34)", *l.c.*, , p. 3 (Question 22).

[973] C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 78. See also HL Deb, 5 July 1983, vol. 443, at cc 509, accessible at http://hansard.millbanksystems.com/lords/1983/jul/05/data-protection-bill-hl#S5LV0443P0_19830705_HOL_103

[974] C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 78. See also HL Deb, 5 July 1983, vol. 443, at cc 509-510, accessible at http://hansard.millbanksystems.com/lords/1983/jul/05/data-protection-bill-hl#S5LV0443P0_19830705_HOL_103. In case of non-compliance, the Registrar had the power to issue an enforcement notice (section 10). In principle, such notices could be directed to either data users or computer bureau. For more information on the types of notices which the Registrar might issue see C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 119 et seq.; A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 136 et seq.

[975] C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 78.

[976] *Id*.

[977] K. Wong, "Data Protection Law", *Data Processing* 1984, Vol. 26, no. 1, p. 13.

443. DATA PROTECTION PRINCIPLES – Data users were bound to comply with eight data protection principles enumerated in Schedule 1 of the Act, i.e. the principles of

(1) Fairness and lawfulness;

(2) Purpose specification;

(3) Disclosure and use limitation;

(4) Proportionality;

(5) Accuracy;

(6) Limitation of storage duration;

(7) Data subject rights; and

(8) Security.[978]

As indicated above, only the eighth principle (security) was directly applicable to computer bureaux. The eighth principle read as follows:

> "*Appropriate security measures shall be taken against unauthorized access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.*"

444. REGISTRATION – In its application for registration, a data user was obliged to provide the following pieces of information (section 4(3)):

(1) name and address;

(2) *description of the personal data* to be held by him and of the *purpose(s)* for which the data are to be held or used;

(3) a *description of the source(s)* from which he intends or may wish to obtain the data or the information to be contained in the data;

(4) a description of any *person(s) to whom he intends* or may wish *to disclose* the data;

(5) the names or a description of any *countries* or territories outside the United Kingdom to which he intends or may wish directly or indirectly to transfer the data ; and

(6) one or more addresses for the receipt of *requests from data subjects* for access to the data.

[978] Part II of Schedule 1 of the Act contained interpretative provisions with regard to the data protection principles. For a discussion of the 1984 data protection principles see also C. Edwards and N. Savage, "Data Privacy: the UK Experience", in C. Edwards and N. Savage (eds), *Information Technology & The Law*, Basingstoke, MacMillan Publishers, 1986, p. 126. It is also worth noting section 2(3) enabled the Secretary of State to impose additional requirements or restrictions in relation to sensitive data.

Persons carrying on a computer bureaux were also under an obligation to register their activities with the Data Protection Registrar. However, bureau were only obliged to specify their name and address in their application for registration (section 4(4)).

445. ROLE OF REGISTRATION – Registration under the 1984 Data Protection Act served several important functions. First, registration was designed to enable the Registrar to assess compliance.[979] Second, because the register itself was to be open to the public, it was expected to provide a starting point for data subjects who wished to investigate who held which data on them and why.[980] Finally, section 5 of the DPA obliged data users and their agents to abide by the terms of the registration. Section 5(3) explicitly stated that users and agents alike were bound to comply with any restrictions regarding use, disclosure or transfer of the data resulting from the terms of the registration.[981] For this reason, it was recommended that the contract between users and bureau specify that the user shall be bound to supply the bureau with a copy of the user's register entry in respect of data processed by the bureau, and to keep the bureau informed of any alterations.[982]

446. DATA SUBJECT RIGHTS – The 1984 Data Protection Act provided data subjects with a right of access, correction and erasure (see section 21 and 24). These rights could only be exercised towards the data user. Computer bureaux were under no obligation to comply with such requests.[983]

447. CRIMINAL LIABILITY – The 1984 DPA exposed both data users and computer bureau to the risk of criminal liability. Certain offences could, by definition, only be committed by data users (e.g., "holding" personal data not described in the registry). Other offences could only be committed by a computer bureau (e.g., operating as a computer bureau without being registered). However, many of the offences created by the DPA could be committed by both users and bureaux (e.g., disclosing data other than as described in the register). The 1984 Data Protection Act created the following offences[984]:

---

[979] See section 7 of the DPA.
[980] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 126.
[981] The term "agent" encompasses computer bureaux (see section 1(6).
[982] T. Cook, "The law relating to computer bureaux", *l.c.*, p. 164. According to the Data Protection Registrar, not all computer bureaux needed to know what was contained in the register entry of the data user to whom it was providing services. A computer bureau which only performed the limited service of "causing data to be processed automatically" would not do anything which constituted an offence under section 5(3). If the computer bureaux provided a wider service, however, which involved collecting information on behalf of the data user or disclosing it in accordance with its instructions, it would run the risk of committing an offence if departed from the particulars contained in the user's register entry. See The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", *l.c.*, p. 6 (Question 9).
[983] T. Cook, "The law relating to computer bureaux", *l.c.*, p. 165 and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 122. In fact, computer bureau were generally prohibited from making any disclosure other than those authorized by the data user.
[984] A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 139.

(1) holding personal data *without being registered* (or without having applied for registration) (section 5 (5));

(2) knowingly or recklessly *holding personal data not described* in the register entry (section 5(5));

(3) knowingly or recklessly *using, obtaining, disclosing or transferring* personal data *other than as described* in the register entry (section 5(3) and 5(5));

(4) knowingly or recklessly operating as a computer bureau in respect of personal data without being registered as such (section 5(5));

(5) knowingly or recklessly *disclosing personal data without the authority* of the person to whom computer bureau service are provided (section 15(3));

(6) failure to comply with an *enforcement notice* (section 10(9));

(7) failure to comply with a *transfer prohibition notice* (section 12(10));

(8) knowingly or recklessly supplying the Registrar with *false or misleading information* on an application for registration (or for alteration of a register entry) (section (6));

(9) failure to keep the *registered address* up to date (section 6(5));

(10) intentional *obstruction* of a person executing a search warrant or failure, without a reasonable excuse, to give help reasonably required by a person executing a search warrant (schedule 4 section (12))

The DPA further provided that, in cases where an offence is committed by a corporate body, any director, manager, secretary or similar officer could be found personally guilty of an offence if it was proved that the offence was committed with the "consent or connivance" of the person concerned, or to be attributable to neglect on that person's part (section 20(1)). In such a scenario, both the person concerned as well as the corporate body would be punishable for the offence.[985]

448. CIVIL LIABILITY – The 1984 Data Protection Act provided data subjects with a claim for compensation of damages in two situations, namely (1) in case of damages suffered by reason of inaccuracy of data (section 22); or (2) in case of damages suffered by reason of loss, unauthorized disclosure, or access to data (section 23). While compensation for inaccuracy could only be obtained from the data user, an award for damages in case of a security breach could in principle also be obtained from a computer bureau.[986] According to the Data Protection Registrar, the computer bureau would only

[985] Section 20(2) continued by stating that "Where the affairs of a body corporate are managed by its members subsection (1) above shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate." See also A.C.M. Nugter, *Transborder Flow of Personal Data within the EC*, *o.c.*, p. 139-140.

[986] It is interesting to note that the civil remedies provided by the 1984 Data Protection Act did not cover all data protection principles (effectively only the fifth and eighth principle were covered). For example, there is no provision for compensation in case of unlawfully obtained data or unauthorized use of data.

be liable in so far as the destruction, disclosure or access occurs without the authority of the computer bureau (sic).[987]

1.3 CONCLUSION

449. CONSISTENCY – Despite its long legislative history, the basic concepts underlying the 1984 Data Protection Act remained largely unchanged. From the outset, both the Younger and Lindop Committee recognized the difference between the "users", "operators", and "owners" of computer services. In the end, two distinct roles were recognized: that of the "computer bureau" and that of the "data user". The former was viewed primarily as a facility provider, whereas the latter was considered to be the product beneficiary.[988]

450. FORMAL RECOGNITION OF COMPUTER BUREAUX – The 1984 Data Protection Act was not the first act to recognize the existence of computer bureaux.[989] Nevertheless, the appearance of the term "computer bureau" is noteworthy.[990] The reports of the Younger and Lindop Committees suggest that the recognition of bureaux was mainly a result of lobbying on the part of the UK computer industry. In their contributions, representatives of computer industry eagerly differentiated the providers of computing services from their customers. The main objective was seemingly to ward off any direct responsibility or accountability for their service offerings.

451. ALLOCATION OF RESPONSIBILITY AND RISK – Like the Lindop Committee before it, the House of Lords wound up rejecting the notion that computer bureaux should be left outside the scope of the Data Protection Act. Bureaux would be subject to the Act,

---

This was reportedly a deliberate choice, as policymakers felt that existing civil law remedies (such as torts for breach of confidence, breach of contract or negligence) would be sufficient. Nevertheless, the limited scope of the claims recognized by the DPA was criticized at length by several scholars. See J. McBride, "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)", *l.c.*, p. 544-545 and C. Edwards and N. Savage, "Data Privacy: the UK Experience", *o.c.*, p. 130-131.

[987] The Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", *l.c.*, p. 22 and (note: while the text in both instances states "without the Computer Bureau's authority", one may venture to suggest this was an error and should have read "without the Data User's authority").

[988] See also Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 255.

[989] The first data protection act to regulate computer bureaux as distinct entities was the Danish Private Register Act of 1978 which similarly required "computer service bureaux" to register their activities with the data protection registrar. (See paragraph 20 of the Private Register Act (*lov om private register*) of 8 June 1978 (nr. 293), accessible at http://www.datatilsynet.dk/internationalt/groenland/lov-om-private-registre-mv). The reader may note that the three data protection acts adopted before 1981 which were studied in this thesis (i.e., Hesse, Sweden and France) also contained provisions which were directly applicable to entities processing data "on behalf of" other persons. However, the Danish act of 1978 appears to the first occasion whereby the term "computer service bureau" was explicitly mentioned in a piece of legislation and used to vest such entities with particular responsibilities.

[990] While Convention 108 recognized the existence of computer bureaux in its Explanatory Memorandum, it refrained from formally recognizing them as a separate entity within the body of the Convention. The UK was thus not under any international obligation to provide explicit recognition to this category of entities.

but would have far fewer responsibilities bestowed upon them. Computer bureaux were mainly obliged to (1) register their activities; (2) act in conformity with instructions of the data user as well as the terms of the relevant register entries; and (3) ensure the security of processing. The remainder of the obligations provided under the Act were directed almost exclusively to data users. Nevertheless, bureaux were subject to the supervision of the Registrar and were exposed to the risk of both civil and criminal liability for activities residing within their sphere of control.[991]

452. RECOGNITION OF PLURALISTIC CONTROL – Another notable feature of the 1984 data protection act was its recognition of pluralistic control. Not only did it recognize that control might be exercised by more than one party, it also recognized two different ways in which control might be shared ("jointly or in common").

453. AFTERMATH – The UK Data Protection Act remained largely unmodified until 1998, when it underwent major revisions in order to implement Directive 95/46/EC.[992]

[991] The analysis of the activities of computer bureaux by the Lindop Committee reports suggest that that UK policymakers had a particular relationship and business model in mind when deciding that bureau should be brought within the scope of the act (see Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 252-259).

[992] Data Protection Act 1998, 1998 Chapter 29, accessible at http://www.legislation.gov.uk/ukpga/1998/29.

2 BELGIUM (1992)

2.1 ORIGIN AND DEVELOPMENT

454. EARLY INITIATIVES – The first Parliamentary proposal to introduce data protection legislation in Belgium was submitted in 1971.[993] Many other like-minded proposals would follow, none of which would become law.[994] Throughout the 1970's, the Belgian government showed remarkably little appetite for data protection legislation.[995] Instead, it contented itself with the view that existing laws offered adequate protections and that it should await the outcome of ongoing international initiatives, in particular by the Council of Europe.[996]

455. A PIECEMEAL APPROACH – Beginning in the early 1980's, Belgium began to adopt laws regulating the use of certain categories of data. The scope of application of these laws was, however, strictly limited to a specific sector or database.[997] Most notable were the Law on the National Register[998] (1983) and the Law establishing the Crossroadsbank of Social Security[999] (1990). Both laws imposed substantial restrictions on the extent to which certain information could be used or made available. At the same time, both laws were equally (if not more so) concerned with a desire to legitimate and further facilitate the automated exchange of personal information.[1000]

456. MOUNTING INTERNATIONAL PRESSURE – Belgium had signed Convention 108 of the Council of Europe as early as 1982. Ratification, however, did not take place until 1991.[1001] In the end, the final push for ratification came from growing pressure within the international community.[1002] The Schengen Implementation Agreement[1003] explicitly

---

[993] Voorstel van wet betreffende de bescherming van het privé-leven en de persoonlijkheid, *Parl. St.*, *Senaat*, 1970-1971, 19 juli 1971, nr. 706. The legislative proposal was based on an academic publication by C. Aronstein, "Défense de la vie privée. Essai pour contribuer à la survie de notre civilisation", *Journal des Tribunaux* 1971, p. 453-463. See also P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, published by Commissie voor de Bescherming van de Persoonlijke Levenssfeer, 2013, p. 47 accessible at http://www.anthologieprivacy.be/sites/anthology/files/documents/Anthologie-Privacy-PDH-SG-WDB.pdf (last accessed 11 August 2015).

[994] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 243 (noting that between July 1971 and May 1981 a total nine parliamentary bills and a government bills were brought before the Belgian parliament, none of which were enacted into law).

[995] R. Pagano, "Panorama of Personal Data Protection Laws", *l.c.*, p. 244

[996] F.W. Hondius, *Emerging Data Protection in Europe*, *o.c.*, p. 27

[997] P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 25-26.

[998] Wet van 8 august 1983 tot regeling van een Rijksregister van de natuurlijk personen, *B.S.* 21 april 1984.

[999] Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, *B.S.* 22 februari 1990.

[1000] See P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 34-46 and 54-55.

[1001] Wet van 17 juni 1991 houdende goedkeuring van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981, *B.S.* 30 december 1993.

[1002] P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 57

required Contracting Parties to provide for a level of protection at least equal to that resulting from the principles laid down in Convention 108.[1004] The Schengen obligation, combined with an increasingly negative reputation of Belgium as a "data processing haven", eventually led the Belgian government to ratify Convention 108 and propose comprehensive data protection legislation.[1005]

457. LEGISLATIVE DEVELOPMENT – A first draft of the Belgian Data Protection Act was submitted by the government on 16 May 1991.[1006] Despite repeated calls of urgency, the draft bill still underwent several substantive revisions.[1007] Throughout the legislative debate, a recurring point of criticism was that the bill would require many implementing acts before it could take full effect. The final text of the act was signed into law on 8 December 1992.[1008].

2.2 ALLOCATION OF RESPONSIBILITY AND RISK

458. TERMINOLOGY – Not surprisingly, the terminology of the 1992 Data Protection Act was quite similar to that of Convention 108. The definitions were not, however, identical. For instance, the Belgian definition of the "controller of the file" was notably shorter than its counterpart in Convention 108. The Belgian data protection act also formally recognized the concept of a "processor", which was similar to the concept of the "computer bureau" recognized by the 1984 UK Data Protection Act.[1009]

A. "Controller of the file"

459. FORMAL DEFINITION – Article 1, §6 defined the "controller of the file" (in Dutch: "*houder van het bestand*"[1010]) as

> "*the natural or legal person or association which is competent to decide about the purpose of the processing or about the types of data that shall be included in the processing.*

[1003] Convention implementing Schengen agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 19 June 1990.
[1004] Article 117 of the Schengen Implementation Agreement.
[1005] P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 57. See also Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *Rechtskundig Weekblad* 1992-1993, nr. 34, p. 1145.
[1006] Wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1990-1991, 6 May 1991, nr. 1610-1.
[1007] P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 49 and 56-57
[1008] Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993.
[1009] Cf. *supra*; nr. 434.
[1010] The Dutch term "houder van het bestand" would translated more accurately into English as "the keeper of the file". However, as the term "houder van het bestand" was the official translation of the term "controller of the file" as it appeared in Convention 108, the same English term is used here.

In case the purpose of the processing or the types of data to be included are specified by law, the controller of the file shall be the natural or legal person that is appointed by law to process the data."

460. "NATURAL OR LEGAL PERSON OR ASSOCIATION" – The controller of the file could be either a natural or legal person, or an association (in Dutch: "*feitelijke vereniging*"). The Act in principle applied to both the public and private sector, but it contained exemptions and derogations for certain public sector entities.[1011] The Act also contained an exemption for "*data kept by natural persons, which are intended for private, family or household use and which keep this purpose*" (article 3, §2, 1°).[1012]

461. "COMPETENT TO DECIDE" – The controller of the file was the party "competent to decide" about the processing. The definition thus adopted a *functional approach*, by allocating responsibility for compliance with the party that could exercise final decision-making power with regards to the processing.[1013]

462. "PURPOSE OR TYPES OF DATA" – The second element of the definition concerned the object of the controller's decision-making power. The controller of the file was understood to have decision-making power "about the *purpose* of the processing *or* about the *types of data* that shall be included in the processing".

463. PRIMACY OF PURPOSE – In cases where the actor deciding about the processing was not the same as the actor deciding about the types of data to be processed, it appeared that preference should be given to the actor deciding about the purpose of the processing.[1014] According to the preparatory works, the controller is the *actor who decides to process personal data for a particular purpose*, rather than the technicians who decide which data are necessary to achieve the chosen purpose.[1015]

[1011] F. Robben, "Toepassingsgebied en begripsdefinities", in J. Dumortier en F. Robben, *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, Brugge, Die Keure, 1995, p. 41 (referring to article 3§3 and article 4§1).

[1012] For a discussion see Memorie van Toelichting, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1990-1991, 6 May 1991, nr. 1610-1, p. 7; Verslag namens de Minister van Justitie uitgebracht door Mevr. Merckx-Van Goey, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1991-1992 (B.Z.), 2 juli 1992, nr. 413-12, p. 23; F. Robben, "Toepassingsgebied en begripsdefinities", *o.c.*, p. 35-36 and Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *l.c.,* p. 1147.

[1013] Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *l.c.,* p. 1147 and S. Gutwirth, "De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", *Tijdschrift voor Privaatrecht* 1993, Vol. 4, 14, p. 1443.

[1014] F. Robben, "Toepassingsgebied en begripsdefinities", *o.c.*, p. 43-44.

[1015] Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *l.c.,* p. 1147, with reference to Verslag namens de commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St., Senaat*, 1991-1992 (B.Z.), 27 October 1992, nr. 445-2, p. 52-53.

464. CBPL PROPOSAL – It is worth noting that the Belgian Privacy Commission (CBPL)[1016] had proposed to extend the definition of "controller of the file", to state the controller must also hold decision-making power regarding

(a) the types of processing activities to be performed;

(b) third parties to whom the data might be disclosed; and

(c) the processor to whom the processing of personal data might be entrusted.[1017]

The CBPL justified the proposal by saying that these elements are important aspects of the processing and therefore the controller of the file should also have the power to decide about them.[1018] The government, however, declined to take up the proposal.[1019] It reasoned that in practice the decisions about these aspects might be taken by several different actors. If the proposal of the CBPL were to be adopted, it would lead to situations in which there is no actor that satisfied the definition.[1020]

465. CONTINUED REFERENCE TO "THE FILE" - The decision to keep the term "controller of the file" was heavily criticized.[1021] After all, the Act also covered completely automated processing, which meant that one could be labelled "controller of the file" without an actual "file" being present.[1022] The decision to keep the term "controller of the file" was justified mainly by a desire for consistency with the terminology of Convention 108.[1023]

466. "PROCESSING" AS A SET OF OPERATIONS – The decision-making power of the controller extended to the "processing" of personal data. The term "processing" was defined in the Act as a *set of operations*, as opposed to an individual processing

---

[1016] The Belgian Privacy Commission (in Dutch: "*Commissie voor de Bescherming van de Persoonlijke Levenssfeer*" – CBPL) had previously been established by the Law on the National Register and reformed by the Law on the Crossroadsbank for Social Security. See P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, 45.

[1017] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 7/92 betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 12 May 1992, p. 9.

[1018] *Id.*

[1019] See Verslag namens de Minister van Justitie uitgebracht door Mevr. Merckx-Van Goey, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, Parl. St. Kamer, 1991-1992 (B.Z.), 2 July 1992, nr. 413-12, p. 99-100.

[1020] *Ibid*, p. 100. Article 16, §1, 1° of the Act would, however, require controllers to make an inventory of interconnections between the data as well third parties to whom the data might be disclosed (cf. *infra*).

[1021] See J. Dumortier, "Privacybescherming en gegevensverwerking. Aantekeningen bij de Wet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens", *Vlaamse Jurist* 1993, p. 9 and F. Robben, "Toepassingsgebied en begripsdefinities", *o.c.*, p. 44.

[1022] *Id.* See also Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St., Senaat*, 1991-1992 (B.Z.), 27 october 1992, nr. 445-2, p. 20 ("*De term «houder van het bestand - maître du fichier» werd waarschijnlijk als zodanig behouden omdat het een geijkte term is, maar hij slaat in feite op veel meer dan alleen het bestand. Hij slaat op degene die de verwerking houdt of die daarvoor verantwoordelijk is"*).

[1023] Verslag namens de Minister van Justitie uitgebracht door Mevr. Merckx-Van Goey, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer, 1991-1992 (B.Z.), 2 juli 1992, nr. 413-12, p. 17-18.

operation. A single processing operation did not constitute "processing" within the meaning of the Act.[1024] Instead, the term "processing" referred to the *entirety of operations undertaken for a particular purpose*.[1025] Robben noted early on the practical difficulties that might arise in determining whether a given series of operations should be considered as being part of the same "processing" or not.[1026] Robben argued that "a reasonable balance" should be struck between the following two extremes:

> "*On the one hand, a situation in which practically all operations carried out by an entity are considered as a single "processing" with either a highly generic purpose or numerous sub-purposes. The principle of finality, a basic principle of the law, would then risk being undermined in practice because the data could be used without restriction for many different purposes. Moreover, the description of the processing will be so general as to render effective supervision impossible.*
>
> *On the other hand, a situation in which the entirety of processing operations carried out is heavily divided in to numerous processing activities, which would require submission of a separate notification for each processing activity, with a very precise indication of the specific objectives pursued, each time accompanied by the payment of a fee. In this scenario, the strict application of the principle of finality would completely obstruct the efficiency of data processing and supervisory authorities would be overwhelmed with declarations and any amendments thereto.*"[1027]

Robben concluded that it would be up to the CBPL to articulate the requisite level of precision that would strike the appropriate balance between these two extremes.[1028] The argument made by Robben was based on an argument put forward by Gutwirth, who had previously cautioned against overly broad definitions of purpose.[1029] According to Gutwirth,

> "*The delineation of finality thus embodies the key question for the implementation of the Privacy Act. Pleas for the recognition of 'carte blanche' or 'catch all' finalities threaten to undermine the entire substance of the law. In contrast, a requirement for an extensive specialization or limitation of finalities would however be impracticable and run counter to the spirit of the law, which aimed to create a flexible system.*"[1030]

[1024] J. Dumortier, "Privacybescherming en gegevensverwerking. Aantekeningen bij de Wet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens", *l.c.,* p. 8.
[1025] *Id.*
[1026] F. Robben, "Toepassingsgebied en begripsdefinities", *l.c.*, p. 28.
[1027] *Ibid*, p. 28-29 (loose translation).
[1028] *Ibid*, p. 29.
[1029] S. Gutwirth, "De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", *Tijdschrift voor Privaatrecht* 1993, vol. 4, p. 1458.
[1030] S. Gutwirth, "De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", *l.c.*, p. 1458 (loose translation). For a more recent discussion see S. Gutwirth, *Privacy and the information age*, Rowman & Littlefield Publ., Lanham, 2002, p. 97 ("*Calls for the recognition of 'catch all' purposes threaten*

467. NO FORMAL RECOGNITION OF JOINT CONTROL – Article 1, §6 did not formally recognize the possibility that the decision-making power over the processing might be exercised by more than one actor. To the contrary, the preparatory works clearly indicate that the purpose of the definition was to arrive at a *single* controller for each processing.[1031] Legislative intent notwithstanding, Robben argued that there may well be situations in which it may be impossible to appoint a single controller.[1032] This could occur particularly in cases where different sets of processing activities were wholly or partially integrated with one and other.[1033] In such scenarios, one would have to determine whether it is possible to separate the decision-making power per "sub-processing" (separate control) or it is necessary to view the processing as one "global" processing with joint control.[1034]

468. PROCESSING SPECIFIED BY LAW – Article 1, §6 explicitly provided that in cases where the purpose of the processing or the types of data to be included were specified by law, the controller of the file would be *"the natural or legal person that is appointed by law to process the data."* In such case, the functional approach described above could be discarded.[1035]

B. "Processor"

469. FORMAL DEFINITION – Article 1, §7 defined the "processor" (in Dutch: "*bewerker*")[1036] as

> "*the natural or legal person or association entrusted with the organisation and execution of the processing*".

470. "NATURAL OR LEGAL PERSON OR ASSOCIATION" – The processor could be either a natural or legal, as well as an association (in Dutch: "*feitelijke vereniging*").

---

to undermine the whole legislative framework. Such definitions of finalities as "make profit" or "contribute to whatever is of service to a person or corporation" does not impose any limits whatsoever. Any banker insurer-tour operator-salesperson of personal data can do whatever he/she wants. On the other hand, the demand to have stringent specifications of purposes would become paralyzing and unworkable. It would create a massive amount of red tape. In ideal circumstances, the specific purpose of processing should be defined somewhere in between the two extremes, taking into account the constitutional weight of privacy's freedom and the necessity of a catch-up operation.")

[1031] Verslag namens de Commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St., Senaat*, 1991-1992 (B.Z.), 27 October 1992, nr. 445-2, p. 52 and 123.

[1032] F. Robben, "Toepassingsgebied en begripsdefinities", *o.c.*, p. 45.

[1033] *Id.*

[1034] *Id.*

[1035] *Ibid*, p. 44.

[1036] The term "bewerker" could also be translated as "editor", "adaptor", or "redactor". For purposes of simplicity, I have chosen to use the term "processor" here, even though the proper Dutch counterpart for this term is "verwerker" rather than "bewerker". The justification for doing so is the fact the definition of "bewerker" itself refers to the "processing" ("verwerken") of personal data.

471. CBPL PROPOSAL – The CPBL had proposed to make a further distinction between "processing agents" and "processors". The term "processing agent" would be reserved for entities *outside* the organisation of the controller to whom the processing of personal data has been entrusted. The term "processor", on the other hand, would cover the person *within* the organisation of controller, appointed by the controller to ensure compliance with data protection requirements.[1037] The government declined to take up the proposal, arguing that the distinction was superfluous.[1038]

472. "ORGANISATION AND EXECUTION" – The processor was seen as a "mere executor", acting pursuant to the instructions of the controller of the file.[1039] Differentiating between controllers and processors thus required an assessment of who is actually competent to decide about the processing and those who merely executed the processing.[1040]

C. Civil and criminal liability

473. FINAL RESPONSIBILITY WITH CONTROLLER – The controller of the file carried the final responsibility for compliance, regardless of how the processing was organised.[1041] Even in cases where the controller relies on a processor to execute processing of personal data, the controller would remain liable in case of non-compliance.[1042]

474. CIVIL LIABILITY – The civil liability of the controller resulted primarily from article 1382 Civil Code (general liability in tort). In addition, article 42 of the Data Protection Act provided that the controller of the file shall be liable "*for the payment of fines to which his appointee or agent has been condemned*".

475. CRIMINAL LIABILITY – Articles 38 and 39 imposed criminal penalties in case of violation of several provisions of the Act (e.g., violation of the finality principle, failure to register, etc.). Many of the criminal provisions were explicitly targeted at the controller

---

[1037] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 7/92 betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 12 May 1992, p. 9-11.

[1038] See Verslag namens de Minister van Justitie uitgebracht door Mevr. Merckx-Van Goey, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St. Kamer*, 1991-1992 (B.Z.), 2 July 1992, nr. 413-12, p. 100 (stating there would be no added value in such a distinction). See also F. Robben, "Toepassingsgebied en begripsdefinities", *o.c.*, p. 45-46.

[1039] Verslag namens de commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St., Senaat*, 1991-1992 (B.Z.), 27 October 1992, nr. 445-2, p. 80 ("*De bewerker is maar een uitvoerder*")

[1040] Verslag namens de commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St., Senaat*, 1991-1992 (B.Z.), 27 October 1992, nr. 445-2, p. 52.

[1041] F. Robben, "Toepassingsgebied en begripsdefinities", *l.c.*, p. 41.

[1042] See also Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 7/92 betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 12 May 1992, p. 9.

of the file.[1043] Other provisions had a more general nature ("*he who …*"), which meant they could in principle extend to entities other than the controller.[1044]

476. PROPOSAL OF CBPL – It is worth noting that the CPBL had proposed to extend the scope of several criminal provisions to processors[1045], but the proposal was not followed up.

2.3 CONCLUSION

477. A LATECOMER TO THE DATA PROTECTION SCENE – The Data Protection Act of 1992 has been characterized as a "rush job".[1046] After years of procrastination, the Belgian government suddenly felt an urgent need to adopt general data protection legislation because of growing international pressure. The outcome was a job half done, with many provisions requiring further implementation before they could take effect.[1047]

478. ALLOCATION OF RESPONSIBILITY AND RISK – Similar to Convention 108, the Data Protection Act of 1992 designated the "controller of the file" as the entity ultimately responsible for ensuring compliance. The Act additionally recognized the concept of a "processor", but did very little with it in terms of further regulation. The main purpose of the term was seemingly to reinforce the responsibility of the controller, regardless of how the processing was organized.

479. AFTERMATH - It would take more than two years before the Belgian Data Protection Act would enter into force.[1048] By then, the text of Directive 95/46/EC was almost finalized and the plans for revision of the Act began to materialize.[1049] The Directive was implemented into Belgian law by way of the Law of 11 December 1998.[1050]

[1043] Verslag namens de commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.*, *Senaat*, 1991-1992 (B.Z.), nr. 445-2, p. 37; 54-55 and 80. Although several provisions also make reference to the "representative, appointee or agent" of the controller, the preparatory works make clear that it was the general intent of the Belgian legislator not to impose criminal liability upon processors as such. (*Ibid*, p. 80).

[1044] *Id.* See also Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *l.c.,* p. 1154.

[1045] Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Advies nr 7/92 betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, 12 May 1992, p. 39-40.

[1046] P. De Hert, S. Gutwirth and W. Debeuckelaere, *Anthologie privacy: referentietekst*, *o.c.*, p. 57-58.

[1047] *Ibid*, p. 79-80.

[1048] *Ibid*, p. 66.

[1049] *Ibid*, p. 67.

[1050] Wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *B.S.*, 3 February 1999.

Chapter 6 DIRECTIVE 95/46/EC

1 ORIGIN AND DEVELOPMENT

480. KEEPING UP WITH THE COUNCIL OF EUROPE – At the level of the European Community, official interest in the privacy issues surrounding automated data processing first emerged in 1973. Less than two months after the Council of Europe approved Recommendation 73(22), a Member of the European Parliament inquired whether the European Commission planned to propose any measures to protect the privacy of citizens "in connection with the compilation of data-banks".[1051] At the time, the Commission responded that this was essentially a matter that should be left to the Member States.[1052]

481. ECONOMIC RELEVANCE – On 21 November 1973, the European Commission issued a Communication regarding a "Community Policy on Data Processing".[1053] The Communication stressed the importance of having a flourishing European data processing industry and proposed several measures designed to promote its development.[1054] Although the Communication focused primarily on economic aspects of data processing, it also noted a need to establish "common measures" to protect citizens.[1055] The Commission recommended the organisation of public hearings to seek out "common ground rules", so as to avoid the need for harmonising legislation in the future.[1056]

482. PARLIAMENTARY MOTIONS – In 1975, the Legal Affairs Committee of the European Parliament prepared an "own initiative" report, which contained a draft Resolution calling for a Directive on "individual freedom and data processing".[1057] A Directive was deemed necessary not only for the protection of citizens, but also to avoid the development of conflicting legislation.[1058] The Resolution was passed[1059], but the

---

[1051] Debates of the European Parliament, Report of Proceedings from 12 to 16 November 1973, 1973-1974 Session, *O.J.* Annex No. 168, November 1973, p. 104 (reply to Oral Question 122/73). See also P. Evans, *l.c.*, p. 574 and F. W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 71

[1052] Id.

[1053] Commission of the European Communities, "Community Policy on Data Processing", Communication of the Commission to the Council, SEC(73) 4300 final, 21 November 1973.

[1054] *Ibid*, p. 4.

[1055] *Ibid*, p. 13.

[1056] *Id.*

[1057] Legal Affairs Committee, Interim Report on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, 19 February 1975, *European Parliament Working Documents* 1974-1975, Document 487/74, p. 5. See also F. W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 72-73 and A.C. Evans, "Data Protection Law", *l.c.*, p. 575-576.

[1058] *Id.*

[1059] European Parliament, Resolution of the European Parliament on the protection of the rights of the individual in the face of the technical developments in data processing, *O.J.* 13 March 1975, C 60/48.

European Commission did not put forth any legislative proposals. The call for legislative action was repeated in 1976, 1979 and 1982.[1060] The Commission, however, preferred to await the completion of Convention 108 and then to urge Member States to ratify it.[1061] The Commission hoped that Convention 108 would be "appropriate for the purpose of creating a uniform level of data-protection in Europe.[1062] It did, however, reserve the right to propose legislation if not all Member States were to sign and ratify the Convention within a reasonable timeframe.[1063]

483. THE PUSH FOR HARMONISATION – As the 1980's progressed, it soon became clear that not all Member States were rushing to ratify Convention 108.[1064] In 1985, the European Commission published a White Paper entitled "Completing the Internal Market", which contained a timetable of completion by 1992.[1065] The continued fragmentation of national approaches to data protection presented a clear risk to the European vision of further integration.[1066] The political push for greater harmonisation provided optimal conditions for further Community action.[1067] In September 1990, the European Commission announced a series of proposed data protection measures, one of which was a proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data.[1068]

484. LEGISLATIVE DEVELOPMENT – The Commission proposal was met with mixed reviews.[1069] After almost two years of debate, the European Parliament published its first reading of the proposal, which contained more than 100 amendments.[1070] The

---

[1060] See European Parliament, Resolution of the European Parliament on the protection of the rights of the individual in the face of the technical developments in data processing, O.J. 3 May 1976, C100/27; O.J. 5 June 1979, C 140/34-38 and O.J. 5 April 1982, C87/39-41. See also D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 22. See also E. Kosta, *Unravelling consent in European data protection legislation: a prospective study on consent in electronic communications*, Doctoral Thesis, Submitted 1 June 2011, p. 88.

[1061] Commission of the European Communities, Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, O.J. 29 August 1981, L 246/31. The Commission was not, however, completely inactive on the topic: see C. Layton, "Protection of Privacy – Future Prospects at the European Communities Level", in OECD, "Transborder Data Flows and the Protection of Privacy", *Information Computer Communications Policy*, nr. 1, 1979, OECD, Paris, p. 213-216.

[1062] Commission of the European Communities, Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, O.J. 29 August 1981, L 246/31. See also See also D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 22-23 and E. Kosta, *Unravelling consent in European data protection legislation: a prospective study on consent in electronic communications*, *o.c.*, p. 88-89.

[1063] *Id.*

[1064] D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 23.

[1065] Commission of the European Communities, "Completing the Internal Market", White Paper from the Commission to the European Council, COM(85) 310 final, 14 June 1985.

[1066] D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 23.

[1067] *Id.*

[1068] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, SYN 287 and 288, 13 September 1990.

[1069] D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 24-25.

[1070] European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in

Commission responded swiftly, releasing an amended proposal for the Directive six months later.[1071] The text was then transmitted to the Council, where the further progression of the document was delayed for more than two years due to a blocking minority.[1072] The political climate eventually changed, however, and on 20 February 1995 the Council reached a common position.[1073] The Parliament's second reading followed soon thereafter.[1074] On 18 July 1995, the Commission issued a favourable Opinion on the Parliament's proposed amendments, which had been relatively minor.[1075] The final version of the Directive was officially adopted on 24 October 1995.[1076]

relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading) *O.J.* 13 April 1992, C 94/173-201.

[1071] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/30-61.

[1072] See D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 26-28.

[1073] Council of the European Union, Common position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/.../EC of the European Parliament and of the Council of ... on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* 13 April 1995, C 93/1-24.

[1074] European Parliament, Decision of the European Parliament on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (C4-0051/95 - 00/0287(COD)), *O.J.* 3 July 1995 C 166/105-107.

[1075] Commission of the European Communities, Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (95) 375 final-COD287, 18 July 1995.

[1076] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, *O.J.* 23 November 1995, L 281/31.

2 ALLOCATION OF RESPONSIBILITY AND RISK

485. OUTLINE – Part II of this thesis provided an in-depth analysis of the allocation of responsibility and risk under Directive 95/46/EC.[1077] The present chapter is limited to a study of how the controller-processor model evolved during the preparatory works leading up to Directive 95/46/EC.

2.1 LEGISLATIVE DEVELOPMENT

A. Commission Proposal

486. "CONTROLLER OF THE FILE" – The starting point for the definitions contained in the Commission proposal were the definitions of Convention 108.[1078] Article 2(e) of the Commission Proposal defined the "controller of the file" as

> "*the natural or legal person, public authority, agency or other body competent under Community law or the national law of a Member State to decide what will be the purpose of the file, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them*"

This definition is identical to the one contained in Convention 108, save for two adaptations:

> "*firstly by referring to Community Law in order to cover the case where specific directives contain substantive provisions on the protection of personal data; and secondly, by specifying that the person who authorizes consultation, notably in the event of direct interrogation, is the controller of the file*".[1079]

487. PERSONS WHO "CONTROL THE OPERATIONS" – Article 18 of the Commission Proposal contained a number of provisions designed to promote *data security*. According to article 18(4), responsibility for compliance with these obligations was not limited to the controller of the file:

> "*The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who, either de facto or by contract, control the operations relating to a file.*"

[1077] Cf. *supra*; nrs. 64 et seq.

[1078] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, *l.c.*, p. 19 ("*The definitions are taken from Council of Europe Convention N° 108 with such adjustments and clarifications as are necessary to guarantee a high level of equivalent protection in the Community*.").

[1079] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, *l.c.*, p. 20. Compare *supra*; nr. 396.

The Explanatory Memorandum clarifies the meaning of article 18(4) as follows:

> "*Article 18(4) assigns responsibility for compliance with the obligations laid down by Article 18(1) to (3). The persons who – de facto or by contract – control the operations relating to a data file are also responsible for ensuring compliance with data security requirements. Those to whom this rule applies are, as the case may be, the controller of the file, the user having access via on-line data retrieval and data processing service bureaux performing data processing on behalf of the controller of the file.*"[1080]

488. PERSONS WITH ACCESS – Article 18(5) provided that

> "*Any person who in the course of his work has access to information contained in files shall not communicate it to third parties without the agreement of the controller of the file.*"

The aim of this provision was to impose a *duty of professional secrecy* on employees of the controller of a file and other persons who in the course of their professional activity have access to personal information contained in a file.[1081]

489. PROCESSING "ON BEHALF OF" – Like Convention 108, the Commission proposal did not define the concept of a "service bureau" or "processor". It did, however, contain a provision dealing specifically with the situation in which the controller enlisted another person to process personal data on its behalf:

> "*Article 22*
> *Processing on behalf of the controller of the file*
>
> *1. The Member States shall provide in their law that the controller of the file must, where processing is carried out on his behalf, ensure that the necessary security and organisational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.*
>
> *2. Any person who collects or processes personal data on behalf of the controller of the file shall fulfil the obligations provided for in Article 16 and 18 of this Directive.*
>
> *3. The contract shall be in writing and shall stipulate, in particular, that the personal data may be divulged by the person providing the service or his employees only with the agreement of the controller of the file.*"

The Explanatory Memorandum clarifies the rationale behind article 22 as follows:

> "*The object of this article is to avoid a situation whereby processing by a third party on behalf of the controller of the file has the effect of reducing the level of protection*

[1080] *Ibid*, p. 38.
[1081] *Ibid*, p. 39.

enjoyed by the data subject. To that end, obligations are placed both on the controller of the file and on the third party carrying out the processing."[1082]

490. LIABILITY – Article 21 provided that any individual who suffers damage as result of any act incompatible with the Directive should be entitled to compensation from the controller of the file. The controller of the file would not be liable for any damage resulting from the loss or destruction of data or from unauthorized access if he could prove that he had taken "appropriate measures" to comply with requirements of articles 18 and 22.[1083]

491. SANCTIONS – Article 23 called on Member States to provide for "dissuasive sanctions", in order to ensure compliance with the measures taken pursuant to the Directive. The Explanatory Memorandum explicitly envisaged *criminal sanctions*, bearing in mind that "non-compliance with data protection principles constitutes infringement of a fundamental right".[1084]

492. ASSESSMENT – The Commission proposal displayed several notable features. The first feature concerns its use of the term "control". The Commission proposal did not consider that the "controller of the file" was the only entity that could exercise "control" over processing operations. "Control over processing operations" could be exercised either by the controller of the file, a person accessing data online, or a service bureau. It seems therefore that the Commission was using the term "control" in an operational sense rather than in a legal sense (i.e., as a legal term of art). A second notable feature of the Commission proposal was the allocation of responsibility contained in article 22(2). This provision provided that any person collecting or processing personal data "on behalf of" the controller was responsible not only to ensure data security (article 18), but also to ensure compliance with the basic data protection principles (article 16) (!). The controller would, however, remain liable for any actions for damages (article 21).[1085] Finally, it is worth noting that, in comparison to Convention 108, the Commission proposal introduced several new elements, such as the obligation for controllers to exercise due diligence when entrusting the processing of personal data to a third party, as well as the obligation to put in place a contract binding provider of the processing service to the controller's instructions.

[1082] Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, *l.c.*, p. 40.

[1083] *Id.*

[1084] *Id.*

[1085] See also recital (20): "*Whereas, in the event of non-compliance with this Directive, liability in any action for damages must rest with the controller of the file; whereas dissuasive sanctions must be applied in order to ensure effective protection*".

B. *First reading European Parliament*

493. OUTLINE –The European Parliament's first reading introduced several important amendments to the original Commission proposal. A first important change was the removal of the old-fashioned concept of the "file", on the grounds that it was outdated and irrelevant given the development of automation and telecommunications.[1086] The "controller of the file" thus became the "controller of the data". A second important change was the formal recognition of the "processor", which had only been implicitly recognized by the Commission's first proposal. Finally, the European Parliament also introduced the definition of a "third party", to designate potential recipients of information that did not belong to the organisation of the controller.

494. "CONTROLLER OF THE DATA" – In its first reading, the European Parliament proposed to define the "controller of the data" as

> "*the natural or legal person, public authority, agency or other body, which processes personal data either on its own account or by a processor and is competent to decide the purpose or purposes for which the personal data are processed, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them.*"[1087]

495. "PROCESSOR" – Article 2(ea) defined a processor as

> "*a natural or legal person who processes personal data on behalf of the controller of the data*".[1088]

Neither Convention 108 nor the OECD Guidelines had adopted the term "processor".[1089] The main reason why the EU legislator decided to introduce this concept was to

> "*avoid situations whereby processing by a third party on behalf of the controller of the file has the effect of reducing the level of protection enjoyed by the data subject*".[1090]

[1086] See Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 3.

[1087] European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading) OJ 13 April 1992, C 94/177.

[1088] *Ibid*, p. 177.

[1089] Although neither Convention 108 nor the OECD Guidelines formally defined the concept of a processor, it is worth observing that the Explanatory Memorandum to the OECD Guidelines did stipulate that a data controller should not be relieved of its obligations merely because the processing of data is carried out on his behalf by another party, such as a "*service bureau*" (see the Explanatory Memorandum to the OECD Guidelines, at paragraph 62). See also *supra*; nr. 371. The Explanatory Report accompanying Convention 108 also indicated that concept of the "controller of the file" did not extend to "*persons who carry out the operations according to the instructions given by the controller of the file*". (Explanatory Report, paragraph 32.) See also *supra*; nr. 400.

496. "THIRD PARTIES" – Article 2(hb) defined third parties as

> "*natural or legal persons other than the controller of the data. The following shall not be considered third parties: employees of the companies which hold the data, to the exclusion of those in their branches, or in companies belonging to the same holding company, if they receive such data in the course of their work.*"[1091]

The definition of the term "third parties" was introduced at the same time as the definition of the term "communication", which was defined by article 2(da) as:

> "*the dissemination, disclosure, transmission or making available of personal data to a natural or legal person; communication shall not include the dissemination or making available of personal data to other persons within the organisation or undertaking in which the controller of the data operates, if such persons receive such data in the course of their duties within the framework of the principles laid down in Article 8(1) hereafter.*"

497. PERSONS WHO "CONTROL THE OPERATIONS" – Article 18(4) was identical to the initial Commission proposal, except that the reference to the "file" was replaced with a reference to "data".[1092]

498. PERSONS WITH ACCESS – Article 18(5) likewise remained unchanged save for the substitution of "file" and "data".[1093]

499. PROCESSING "ON BEHALF OF" - Article 22 underwent two notable changes. First, article paragraph 22(1) made reference to the newly coined term "processor" to refer to persons that process personal data on behalf of the controller of the data. Second, article 22(2) no longer specified that persons acting "on behalf of the controller" were required to fulfil the obligations of former articles 16 (principles) and 18 (security). Instead, the revised article 22(2) simply provided that

> "*The processor shall only carry out that processing of personal data laid down contractually by the controller of the data and shall take instructions only from the controller.*"[1094]

[1090] Commission of the European Communities, "Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data", SYN 287, Explanatory Memorandum, p. 40. The decision to incorporate a separate definition of "processors" was not included in the Commission's initial proposal, but was later introduced pursuant to an amendment proposed by the Committee on Legal Affairs and Citizens' Rights (see Committee on Legal Affairs and Citizens' Rights, Report concerning the proposal by the Commission to the Council for a Directive concerning the protection of individuals in relation to the processing of personal data, European Parliament Session Documents, A3-0010-92, 15 January 1992, 11, amendment nr. 18). See also Opinion 1/2010, *l.c.*, p. 24.

[1091] *Ibid*, p. 177.

[1092] *Ibid*, p. 191 ("*The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who, either de facto or by contract, control the operations relating to data*").

[1093] *Ibid*, p. 191. (""*Any person who in the course of his work has access to information shall not communicate it to third parties without the agreement of the controller of the data").*

[1094] *Ibid*, p. 192.

Article 22(3) still provided that the contract between the controller of the data and the processor must stipulate that personal data may be divulged only with the agreement of the controller of the data.

500. LIABILITY AND SANCTIONS – Article 21 was revised to read as follows:

> "*1. The Member States shall provide in their law that any individual whose personal data have been stored and who suffers damage as a result of unlawful processing or of any act incompatible with this directive shall be entitled to compensation from the controller of the data.*
>
> *2. The controller of the data shall compensate the data subject for <u>any damage resulting from storage of his personal data that is incompatible with this directive</u>."*[1095]

The Parliament's change had the effect of removing the "escape clause" contained in the first draft of article 21, which provided that the controller would not be liable for any damage resulting from the loss or destruction of data or from unauthorized access if he could prove that he had taken "appropriate measures" to comply with requirements of articles 18 and 22 ("security" and "processing on behalf of the controller").[1096]

501. SANCTIONS – Article 23 underwent only minor revisions[1097]

C. Amended EC Proposal

502. OUTLINE – The European Commission took on board many of the changes proposed by the European Parliament, but also added a few (minor) changes of its own. First, the definition of a "controller" was simplified. The Commission proposed to simply refer to the "controller" and to omit any reference to either "the file" or the "data".[1098] Second, the amended proposal added the term "objective", as being an additional aspect decided by the controller. The definition of "processor" remained essentially unchanged. Interestingly, article 17(4) no longer referred to persons "who control the operations", but instead to "persons who share responsibility for carrying out the processing". This change implicitly signalled that the term "control" was no longer being used in an operational sense, but rather as a legal term of art. The most noteworthy change made by the European Commission related article 24(2), which now provided that processors

---

[1095] Ibid, p. 192.
[1096] Cf. *supra*; nr. 126.
[1097] Article 23 was mainly to underline its applicability to both public and private sector entities: "*Each Member State shall make provision in its law for the application of dissuasive sanctions, applicable to both authorities and organisations governed by public law and other natural or legal persons, in order to ensure compliance with the measures taken pursuant to this directive.*"
[1098] The definition was further shortened by referring to the entity "*who processes personal data or causes it to be processed*" (instead of: "*which processes personal data either on its own account or by a processor*") and who "*decides*" (instead of: "*is competent to decide*").

were obliged to comply with *all* of the national provisions adopted pursuant to the Directive (!).

503. "CONTROLLER" – Article 2(d) of the amended EC proposal defined the "controller" as

> "*any natural or legal person, public authority, agency or other body who processes personal data or causes it to be processed and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them*".[1099]

The accompanying Explanatory Memorandum clarified the change as follows:

> "*[A]s the Directive sets out to regulate the use of data in light of the object being pursued, it is preferable to speak of the "controller", and to drop any reference to a "file" or "data".*
>
> *The controller is the person ultimately responsible for the choices governing the design and operation of the processing carried out (usually the chief executive of the company), rather than anyone who carries out processing in accordance with the controller's instructions. That is why the definition stipulates that the controller decides the "objective" of the processing. […] The controller may process data himself, or have them processed by members of his staff or by an outside processor, a legally separate person acting on his behalf."*[1100]

504. "PROCESSOR" – The definition of processor remained the same, save for the change in reference to the "controller" instead of the "controller of the data".[1101]

505. "THIRD PARTY" – The definition of "third party" was modified in order to read:

> "*any natural or legal person other than the data subject, the controller and any person authorized to process the data under the controller's direct authority or on his behalf*".[1102]

According to the Explanatory Memorandum, the definition was reworded in order to clarify which entities should or should not considered as "third parties". As such, persons working for a separate organisation, even if they belong to the same group or holding companies would be considered "third parties". On the other hand, branches

[1099] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311, p. 39.
[1100] *Ibid*, p. 10.
[1101] *Ibid*, 39.
[1102] *Id*.

processing customer information under the direct authority of their headquarters would not be considered third parties.[1103]

506. PERSONS WHO "CARRY OUT THE PROCESSING" – Article 17(4) [former article 18(4)] now provided that the obligations regarding security of processing

> "*shall also be incumbent on persons who share responsibility for carrying out the processing, and, in particular, on the processor.*"[1104]

507. PERSONS WITH ACCESS – Article 17(5) [former article 18(5)] remained essentially unchanged.[1105]

508. PROCESSING "ON BEHALF OF" – Article 24(1) [former article 22(1)] still imposed the same duty of "due diligence" upon controllers, by stating that the controller

> "*must, where processing is carried out on his behalf, ensure that the necessary security and organisational measures are taken and choose a processor who provides sufficient guarantees in that respect.*"

Article 24(2) [former article 22(2)] was revised to stipulate that

> "*The processor shall carry out only such processing of personal data as is stipulated in his contract with the controller and shall take instructions only from the latter. He shall comply with the national provisions adopted pursuant to this Directive.*"

The Explanatory Memorandum elaborates as follows:

> "*In accordance with Parliament's wishes, paragraph 2 emphasizes that the processor may only act within the terms of his contract with the controller. It is proposed that an express reference should be made to the obligations imposed by the national measures taken under the Directive, which shall also apply to a processor.*"

Article 24(3) [former article 22(3)] remained essentially unchanged.[1106]

[1103] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 11.

[1104] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/51.

[1105] *Ibid*, p. 51. It merely added an exception to the general prohibition of disclosure without authorisation of the controller: "*Any person who, in the course of his work, has access to personal data shall not disclose it to third parties without the controller's agreement, unless he is required to do so under national or Community law.*" See also Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 27-28.

[1106] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/54 The changes made appear to have been mainly stylistic: "*The contract shall be in writing and shall state, in particular, that*

509. LIABILITY – Notwithstanding the European Parliament's proposals to amend article 21, the European Commission still felt that Member States should feel free to exempt the controller from liability where suitable security measures were taken.[1107] Articles 23 [former article 21] of the amended proposal provided that

> *"1. Member States shall provide that any person whose personal data are undergoing processing and who suffers damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this directive is entitled to receive compensation from the controller for the damage suffered.*
>
> *2. Member States may provide that the controller may be exempted, in whole or in part, from his liability for damage resulting from the loss or destruction of data or from unauthorized access if he proves that he has taken suitable steps to satisfy the requirements of Articles 17 and 24."*[1108]

510. SANCTIONS – Article 24 [former article 23] underwent minor revisions, which were mainly stylistic in nature.[1109]

D. Council Position

511. OUTLINE – After almost three years of deliberation, the Council text brought with it several significant changes. First, the Council shortened the definition of a "controller" considerably, by referring only to the "*purposes and means of the processing of personal data*" as being the defining object of a controller's decision-making power.[1110] The definition of "processor" underwent minor revisions, essentially to make clear that a

---

personal data processed there under may be disclosed to a third party by the processor or his employees only with the controller's agreement."

[1107] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 33.

[1108] Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/54. See also Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 33.

[1109] Article 24 now provided that "*Each Member State shall provide for the imposition of dissuasive penalties on any person who does not comply with the national provisions adopted pursuant to this Directive*". (Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/55.)

[1110] In the amended Commission proposal, the object of the controller's decision-making power extended not only to the purpose of the processing, but also to (1) objective of the processing; (2) which personal data are to be processed; (3) which operations are to be performed upon them; and (4) which third parties are to have access to them. It would appear that the term "objective" was subsumed the "purpose" of the processing; whereas the question of which personal data are to be processed, which processing operations are to be performed and which third parties are to have access to them were subsumed by the "means" of the processing.

"public authority, agency or any other body" could also act as a "processor". The most drastic changes were introduced via articles 16 and 17 of the Council text. The Council revised these provisions so that *none* of the obligations contained in the Directive would be directly incumbent upon processors. Instead, the source of the processors obligations would result from a "*contract or legal act binding the processor to the controller*".[1111] Finally, the Council text expanded the liability escape clause of article 23(2) to any case where the controller can prove that he is not responsible for the event giving rise to the damage.

512. "CONTROLLER"- In the Council text, article 2(d) defined the "controller" as

> "*the natural or legal person, public authority, agency or any other body which determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by a national or Community law.*"[1112]

513. "PROCESSOR" – Article 2(e) defined the "processor" as

> "*the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*".[1113]

514. "THIRD PARTY" – Article 2(f) defined a "third party" as

> "*the natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data*".[1114]

515. "RECIPIENT" – Article 2(g) defined a "recipient" as

> "*the natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients*"

The term "recipient" was reportedly introduced primarily to help ensure transparency of processing towards data subjects.[1115]

[1111] By doing so, the Council effectively quashed the notion that a processor might have an independent obligation to assess whether its processing activities were in compliance with the requirements of the Directive.

[1112] Council of the European Union, Common position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/.../EC of the European Parliament and of the Council of ... on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. 13 April 1995, C 93/7.

[1113] *Ibid*, p. 7.

[1114] *Ibid*, p. 7.

[1115] *Ibid*, p. 22. Articles 10 and 11, for instance, required controllers to inform data subjects of the "recipients or categories of recipients" of their personal data.

516. PERSONS WITH ACCESS – Article 16 [former article 17(5)] provided that

"*Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.*"

517. DUE DILIGENCE – Article 17(2) [former article 24(1)] provided that

"*the controller must, where processing is carried out on his behalf, choose a processor who provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and must ensure compliance with those measures*".[1116]

518. LEGAL BINDING – Article 17(3) and 17(4) [former articles 24(2) and 24(3)] provided that

"*3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
– the processor shall act only on instructions from the controller,
– the obligations set out in paragraph 1 , as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."[1117]

519. LIABILITY – Article 23 provided that

"1. *Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.*

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage."[1118]

The recitals in the Council text made clear that article 23(2) referred inter alia to situations in which the damages resulted from an "*error on the part of the data subject*" or "*in a case of force majeure*".[1119]

[1116] *Ibid*, p. 12.
[1117] *Ibid*, p. 12. Article 17(1) concerned the controller's obligation to ensure security of processing.
[1118] *Ibid*, p. 14.
[1119] *Ibid*, p. 6.

520. SANCTIONS – Article 24 provided that

> "*The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.*"

E. Second reading and final text

521. OUTLINE – The European Parliament's second reading contained very few amendments. One very important change, however, was the amendment that introduced the notion of "joint control" in the definition of a "controller".

522. CONTROLLER - In its second reading, the European Parliament defined the controller as

> "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or Regulations, the controller or the specific criteria for his nomination may be designated by a national or Community law*".[1120]

The accompanying Explanatory Memorandum provided the following rationale for the change:

> "*Article 2, sub d) is important, because it allows to establish who is subject to the requirements of the Directive. The text appears to relate only to the most prevalent situation, whereby only one person is considered a controller. In practice it may occur, however, that several different persons decide to process personal data for a particular purpose or in the context of permanent relationship (e.g., within a collaboration framework or a professional association) and provide themselves with the necessary technical means to do so. In such a case, each of these persons, as soon as they do not operate as part of the same legal entity, shall be considered a joint controller. This situation may occur more and more in the future, for example in case of an exchange of data between governments or between companies in the context of telematics networks.*"[1121]

[1120] European Parliament, Decision of the European Parliament on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (C4-0051/95 - 00/0287(COD)), O.J. 3 July 1995 C 166/106.

[1121] Commissie juridische zaken en rechten van de burger, "Aanbeveling voor de tweede lezing betreffende het gemeenschappelijke standpunt van de Raad met het oog op de aanneming van de richtlijn van het Europese Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (C4-00051/95 – 00/0287(COD)), PE 212.057/def, A4-0120/95, 24 mei 1995, p. 15 (personal translation of the Dutch official translation).

In its Opinion following the Parliament's second reading, the European Commission reasoned that

> "*Amendment No 3 provides in Article 2(d) for the possibility that for a single processing operation a number of parties may jointly determine the purpose and means of the processing to be carried out. It follows from this that, in such a case, each of the co-controllers must be considered as being constrained by the obligations imposed by the directive so as to protect the natural persons about whom the data are processed.*" [1122]

The European Parliament did not propose any further amendments directly affecting the concepts of "controller", "processor", "third party", "recipient" or the relationship between these entities. The amendments proposed by the European Parliament in its second reading were received favourably by both Commission and the Council. The final text of the Directive 95/46 was officially adopted by the Parliament and Council on 24 October 1995.

2.2 CONCLUSION

523. CONSOLIDATION AND INNOVATION – The main objective of Directive 95/46 was to further harmonize data protection legislation across EU Member States. For the most part, the Directive relied upon the acquis of Convention 108, which had already consolidated the basic architecture for national data protection laws in the EU. However, Directive 95/46 also introduced a number of new elements, in comparison to its predecessor. Important changes included rules on applicable law, the introduction of the concept of processor and the recognition of joint control.

524. ALLOCATION OF RESPONSIBILITY AND RISK – Within the regulatory scheme of the Directive, the controller carries the primary responsibility for ensuring compliance. At the moment of its enactment, the EU legislature was mindful of the practice whereby one organisation requests another organisation to perform certain processing operations on its behalf. By introducing the concept of a "processor", the EU legislator hoped to be able to address this situation and to ensure a continuous level of protection.

525. VARYING DEGREES OF CONTRACTUAL FLEXIBILITY – Directive 95/46 has devoted several provisions to the relationship between controllers and processors. Article 17(3) obliges controllers to conclude a contract with their processors, which must specify that the processor is obliged (1) to follow the controller's instructions at all times and (2) to implement appropriate technical and organisational measures to

[1122] Commission of the European Communities, Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (95) 375 final-COD287, 18 July 1995, p. 3.

ensure the security of processing. In contrast, Directive 95/46/EC in principle does not contain any specific requirements aimed at regulating the relationship among controllers as such.

Chapter 7 GENERAL DATA PROTECTION REGULATION

1 ORIGIN AND DEVELOPMENT

526. REVIEW OF DIRECTIVE 95/46 – For almost 15 years, Directive 95/46 stood strong as the central instrument of data protection regulation in the EU. The European Commission assessed its implementation in 2003 and 2007, both times concluding there was no need for revisions.[1123] In 2010, however, the Commission announced that the time for revisions had come.[1124] The Commission argued that while the objectives and principles underlying Directive 95/46 remained sound, revisions were necessary in order to meet the challenges of technological developments and globalisation.[1125]

527. A CHANGING ENVIRONMENT – Formal preparations for the review began in July 2009, when the European Commission launched a public consultation "on the legal framework for the fundamental right to protection of personal data".[1126] The consultation revealed concerns regarding the impact of new technologies on data protection, as well as a desire for a more comprehensive and coherent approach to data protection.[1127] Perhaps more significantly, 2009 was also the year when the Lisbon Treaty entered into force.[1128] Article 16 of the Lisbon Treaty provided the EU with a legal basis to enact comprehensive data protection legislation across Union policies (including in the area of police and judicial cooperation in criminal matters).[1129] It also

---

[1123] See European Commission, "Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC)", 15 May 2003, COM (2003) 265 final, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0265&from=EN and European Commission, Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive, 7 March 2007, COM (2007)87 final, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0087&from=EN (last accessed 16 October 2015).

[1124] European Commission, "A comprehensive approach on personal data protection in the European Union", Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 4 November 2010, accessible at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[1125] *Ibid*, p. 3.

[1126] European Commission, "Review of the data protection legal framework", accessible at http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm. The public consultation ran from 9 July 2009 to 31 December 2009. For a summary see: European Commission, "Summary of replies to the public consultation about the future legal framework for protecting personal data, 4 November 2010", accessible at http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf (last accessed 15 October 2015). A compilation of the responses received is accessible at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm.

[1127] *Ibid*, p. 4.

[1128] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, O.J. C 306, 17 December 2007.

[1129] European Commission, "A comprehensive approach on personal data protection in the European Union", *l.c.*, p. 4 and 13. See also P. Hustinx, "Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations", speech delivered by Peter Hustinx at the 11th Conference on Data

gave the right to data protection renewed prominence: the right to data protection was recognized both by article 16 of the Treaty and article 8 of the EU Charter of Fundamental Rights, which became legally binding as the Lisbon Treaty entered into force.[1130]

528. PUSH FOR (EVEN) GREATER HARMONISATION – A new public consultation ensued following the EC Communication of 4 November 2010.[1131] The Commission concluded that many stakeholders supported the idea of further harmonisation of data protection rules at EU level.[1132] The Commission also felt that despite its aim, Directive 95/46 had failed to ensure an equivalent level of protection throughout the EU.[1133] Persistent fragmentation meant legal uncertainty, administrative burden and an uneven protection for individuals.[1134] A Regulation would provide a strong and uniform legislative framework at EU level.[1135]

529. CENTRAL THEMES OF THE REFORM – In 2012, the European Commission indicated that the reform of the EU data protection framework would consist of four main elements, namely:

a) To *provide individuals with control* over their personal data (by reinforcing existing data subject rights and adding new rights such as a "right to be forgotten" and a "right to data portability");

Protection and Data Security, Berlin, 8 June 2009, accessible at https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/SA2009 (last accessed 16 October 2015) and C. Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Bloomberg BNA, Privacy and Security Law Report*, 2 June 2012, p. 2.

[1130] *Id.* For a more detailed discussion of the implications of this development see G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014, p. 230 et seq. and H. Hijmans, *The European Union as a constitutional guardian of internet privacy and data protection*, Academisch proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam en de Vrije Universiteit Brussel, 2016, p. 180 et seq., accessible at http://dare.uva.nl/document/2/169421.

[1131] The public consultation on "the Commission's comprehensive approach on personal data protection in the European Union" ran from 4 November 2010 to 15 January 2011. For a summary of the contributions received see Annex 4 to the Commission's Impact Assessment accompanying its initial proposal for General Data Protection Regulation, accessible at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed 16 October 2015), p. 54-73. A compilation of the responses received is accessible at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm.

[1132] European Commission, "Summary of Replies to the Public Consultation on the Commission's Communication on comprehensive approach on personal data protection in the European Union, Annex 4, p. 64.

[1133] European Commission, "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, COM(2012) 9 final, 25 January 2012, p. 7, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en (last accessed at 17 October 2015).

[1134] *Id.*

[1135] *Id.*

b) To render data protection rules fit for the *digital single market* (by providing full harmonisation by a way of Regulation as well as a "one stop shop" mechanism for business);

c) To enable a smoother exchange of personal data in the *area of police and criminal justice co-operation* (by replacing Framework Decision 2008/977/JHA [1136]with a directive); and

d) To develop updated rules for *cross-border data transfers* (for example, by formally recognizing alternative transfer mechanisms such as Binding Corporate Rules).[1137]

530. LEGISLATIVE DEVELOPMENT – The Commission officially released its initial proposal for a General Data Protection Regulation (GDPR) on 25 January of 2012.[1138] The proposed GDPR was accompanied by a proposal for a Directive setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities (Law Enforcement Directive).[1139] After more than two years of intense lobbying, the European Parliament completed its First Reading of the GDPR on 12 March 2014. The Council of the European Union reached a consensus on a General Approach on 15 June 2015.[1140] The General Approach agreed by the Council formed the basis for its further negotiations with the European Parliament in the context of its so-called "trilogue" discussions, to which the European Parliament, Council and Commission participate. On 15 December 2015, the political agreement on the proposed data protection reform was

[1136] Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L 350, 30 December 2008, p. 60.

[1137] European Commission, "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century", *l.c.*, p. 4 et seq.

[1138] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), 25 January 2012, accessible at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed 8 February 2015). An earlier of draft of the proposal was widely leaked in November 2011.

[1139] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data , SEC(2012) 72 final, SEC(2012) 73 final, Brussels, 25 January 2012, COM(2012) 10 final, 2012/0010 (COD), available at http://ec.europa.eu/dgs/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf.

[1140] Council of the European Union, "Data Protection: Council agrees on a general approach" (Press Release), 15 June 2015, available at http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection. Actual text: Council for the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 2012/0011 (COD), 9565/15, 11 June 2015, available at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

announced, thus ending the trilogue process.[1141] On 4 May 2016, the GDPR was published in the Official Journal of the European Union.[1142] It will apply from 25 May 2018.

2 ALLOCATION OF RESPONSIBILITY AND RISK

2.1 LEGISLATIVE DEVELOPMENT

A. Commission Proposal

531. PREFACE – The reform package proposed by the European Commission was accompanied by a third evaluation of the implementation of Directive 95/46.[1143] The evaluation highlighted several issues surrounding key concepts of the Directive, including the concepts of "controller" and "processor". First, the Commission observed that divergent national implementations persisted.[1144] According to the Commission, the lack of a harmonized approach

> "*has led to uncertainties with regard to responsibility and liability of controllers, co-controllers and processors, the actual or legal capacity to control processing, and the scope of applicable national laws, causing negative effects on the effectiveness of data protection.*" [1145]

The Commission also noted that the increased complexity of the environment in which controllers and processors operate (e.g., behavioural advertising, cloud computing) rendered it increasingly difficult to apply the concepts in practice.[1146] In the end,

---

[1141] European Commission, Agreement on Commission's EU data protection reform will boost Digital Single Market, Press Release, Brussels, 15 December 2015, available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm (last accessed 31 March 2016).

[1142] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* 4 May 2016, L 119/1.

[1143] European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2 of Commission Staff Working Paper, *Impact Assessment*, SEC(2012) 72 final, 25 January 2012, p. 5-35, accessible at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed 17 October 2015).

[1144] *Ibid*, p. 8 (noting that while a number of national laws closely follow the definition of the "controller", other laws provide for variations. For instance, certain laws focus on the determination of the "purposes" of the processing, either without any reference to the "means" or make reference to the "contents and use" of processing instead of the "means". The definition of "processor" has also not been implemented consistently across Member States.)

[1145] *Ibid*, p. 9.

[1146] *Id.* The difficulties surrounding the application and implications of the controller and processor concepts was also highlighted by certain stakeholder responses to the 2010-2011 public consultation. See e.g., Information Commissioner's Office, "The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union", 14 January 2011, p. 9, accessible at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocom

however, the Commission arrived at the conclusion that the concepts themselves remain valid.[1147] Legislative changes should focus instead on the obligations and implications associated with each concept:

> *"Although the definitions and concepts of "controller" and "processor" remain themselves relevant, they need to be clarified and detailed in specific provisions as regards the obligations, responsibilities and liability of both controllers and processors. Harmonised rules on the responsibilities of data controllers and processors, including the obligation to demonstrate compliance with their obligations, would foster legal certainty. Including in the case of more than one controller and/or processors being involved, it must be clear for the data subject whom to address to in order to exercise his or her rights*".[1148]

i. Definitions

532. MINIMAL CHANGE – The initial Commission proposal replicated the definitions of controller and processor quasi verbatim. Only one change was made to the definition of a "controller", which was now defined by article 4(5) as

> "'*controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law*"

The only change to the definition of the controller was the addition of the word "conditions". The definition of a processor (article 4(6)) remained identical to its counterpart under Directive 95/46.

ii. Obligations

533. OUTLINE – Chapter IV of the Commission proposal sets forth the obligations of controllers and processors. Article 22(1) begins by reaffirming that the controller is the entity which carries responsibility for ensuring compliance. It also describes some of the measures which it must implement to ensure compliance, taking into account "*the debate on the "principle of accountability*".[1149] The responsibility of the controller to ensure compliance is further made explicit in several other provisions, including those

---

moffice_en.pdf and BEUC, "A Comprehensive Approach on Personal Data Protection in the European Union – European Commission's Communication", 24 January 2011, p. 12-13, accessible at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf .

[1147] European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2, *l.c.*, p. 10.

[1148] *Id.*

[1149] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, *l.c.*, p. 10. See also *infra*; nr. 606 et seq.

regarding (a) the principles of data quality (article 5 f)[1150]; (b) data subject rights (articles 11-20); and (c) data protection by design and by default (article 23). Article 24 explicitly addresses the situation of *joint control*. Articles 26 and 27 seek to clarify the position and obligations of processors, mainly by extending upon articles 16 and 17(2) of Directive 95/46/EC.[1151] Perhaps most significantly, the Commission proposal also specifies a range of obligations *relevant to both controller and processor*:

- the obligation to maintain documentation (article 28)
- co-operation with supervisory authorities (article 29);
- the obligation to maintain an appropriate level of data security (article 30);
- the obligation to notify data breaches (article 31)[1152];
- data protection impact assessments (article 33);
- prior authorization (article 34);
- data protection officers (articles 35-37);
- codes of conduct (article 38);
- certification (article 39); and
- international transfers (articles 40-44).

Interestingly, two sets of obligations are *applicable only to the controller*, namely the obligations regarding data protection by design and by default (article 23) and the obligation to notify data breaches to supervisory authorities and data subjects (articles 31 and 32).[1153]

534. RESPONSIBILITY OF THE CONTROLLER – Article 22 of the Commission proposal provides that

> *1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.*

[1150] Article 5(f) provides that personal data must be "*processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation*. (replacing art. 6(2) Directive 95/46: "it shall be for the controller to ensure that paragraph 1 is complied with"). Difference : "*the controller to ensure*" became "*responsibility and liability of the controller who shall ensure and demonstrate for each processing operation the compliance*")

[1151] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, *l.c.*, p. 10.

[1152] As regards the obligation to notify data breaches, a distinction should be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller (article 31(2)).

[1153] It should be noted, however, that while article 31(1) only requires controllers to notify a supervisory authority in case of a security breach, article 31(2) does require processors to immediately notify controllers in case of a breach.

2. The measures provided for in paragraph 1 shall in particular include:

(a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors."

535. JOINT CONTROL – Article 24 of the Commission proposal provides that

"*Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.*"

536. CHOICE OF PROCESSOR – Article 26(1) of the Commission proposal echoes the obligation of article 17(2) of the Directive, which requires the controller to choose a processor "providing sufficient guarantees" in respect of the technical security measures and organisational measures governing the processing to be carried out. A notable change, however, is that the chosen processor must also guarantee that the processing will be carried out in such a way that it "*will meet the requirements of the Regulation and ensure the protection of the rights of the data subject*".

537. LEGAL BINDING – Article 26(2) of the Commission proposal is based on article 17(3) of the Directive, which provides that the processing carried out by a processor must be governed by a contract or legal act binding the processor to certain obligations. The new provision also contains several new elements, however, which must also be included. Specifically, article 26(2) a requires stipulation that the processor shall:

(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;

(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;

(c) take all required measures pursuant to Article 30 [data security]*;*

(d) enlist another processor only with the prior permission of the controller;

(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III.

(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;

(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;

(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.

Article 26(3) requires the controller and processor to document the controller's instructions and the processor's obligations in writing.

538. BOUND BY INSTRUCTIONS – Article 27 of the Commission proposal is based on article 16 of Directive 95/46, with the noteworthy change that the now the possibility of subprocessing is explicitly recognised[1154]:

"*The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.*"

Article 26(4) further clarifies that if a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers (as laid down in article 24).[1155] Article 26(2)d makes clear that sub-processing requires prior permission of the controller.

iii. Liability and sanctions

539. RIGHT TO COMPENSATION AND LIABILITY – Article 77 of the Commission proposal is based on the liability regime of article 23 of the Directive, but displays a number of notable differences. A first significant change is that article 77(1) extends the data subject's right to damages to processors.[1156] It also explicitly addresses the situation where more than one controller or processor is involved in the processing, stipulating that each controller or processor shall be *jointly and severally liable* for the entire amount of the damage:

[1154] See also P. Blume, "Controller and processor: is there a risk of confusion?", *International Data Privacy Law* 2013, Vol. 3, No. 2 p. 143.
[1155] Cf. *supra*; nr. 535.
[1156] Article 75 of the Commission proposal also clearly specifies that individuals have right to judicial remedy against both controllers and processors.

"1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage."

540. EXEMPTIONS - Article 77(3) replicates the escape clause contained in article 23(2) of the Directive, by providing that

"The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage."[1157]

The only difference brought upon by article 77(3) is that it extends the escape clause to processors as well. In this context, it is worth noting that the Commission proposal also incorporates the intermediary liability exemptions contained in the e-Commerce Directive by way of article 3(3), which provides that

"*This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.*"

Currently, the liability exemptions formally do not apply to matters regulated by Directive 95/46 pursuant to article 1(5)b of the e-Commerce Directive.[1158]

541. PENALTIES – Article 78(1) of the Commission proposal is based on article 24 of the Directive and provides that Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation. It further adds that the penalties provided for must be "*effective, proportionate and dissuasive*".[1159]

542. ADMINISTRATIVE SANCTIONS – Article 79 empowers supervisory authorities to issue administrative fines for the offences listed in this provision. Relevant offences include *inter alia*: the absence of an appropriate mechanism to respond to data subject requests (article 79(4)); failure to provide adequate information to data subjects (article 79(5) and processing personal data without a sufficient legal basis (article 79(6)a). Article 79 does not differentiate between controllers or processors. In principle, the fines may be imposed against "anyone who" fails to comply with the relevant

[1157] Recital (118) further clarifies the meaning of article 77(3) in the same way as recital (55) of Directive 95/46.

[1158] See article 1(5)b of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *O.J.* 17 July 2000, L 178/8. For a more detailed discussion of the relationship between the e-Commerce Directive and the Data Protection Directive see *infra*; nrs. 1152 et seq.

[1159] Recital (19) further clarifies that the penalties should be imposed "*to any person, whether governed by private or public law, who fails to comply with this Regulation*".

provisions.[1160] Article 79(2) does provide, however, that the "degree of responsibility" of the natural or legal person shall be taken into account when determining the amount of an administrative fine.

iv. Assessment

543. CONCEPTS INTACT – The proposal of the European Commission left the concepts of controller and processor intact.[1161] As previously signalled in its evaluation report, the Commission considered the concepts themselves to be largely unproblematic.[1162] The proposed changes instead focused on (a) specifying the obligations of each actor in greater detail; (b) defining additional obligations for processors; and (c) addressing the relationship between joint controllers.[1163]

544. MORE DETAILED OBLIGATIONS – The Commission proposal specifies the obligations of controllers and processors in much greater detail in comparison to Directive 95/46.[1164] Most of the additional obligations (e.g. documentation, data protection impact assessment, designation of a data protection officers) originate from the discussions surrounding the "principle of accountability", which essentially requires controllers to implement appropriate measures to ensure compliance and to demonstrate the measures upon request.[1165] Other provisions, such as the principles of data protection by design and data protection by default (article 23) and data breach notification (articles 31 and 32) are complementary to these obligations.

545. PROMINENCE OF THE PROCESSOR – The Commission proposal deals with processors in a far more detailed way than Directive 95/46.[1166] The obligations incumbent upon processors clearly recognize the important role processors can play, not only in maintaining compliance[1167], but also in assessing the impact of the

---

[1160] Article 73 (right to lodge a complaint) also does not specify whether a complaint might be lodged against either controllers or processors.

[1161] The Commission only proposed one minor change to definition of a controller, namely adding the word "conditions". See also P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review* 2012, vol. 28, p. 133 and P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143.

[1162] Cf. *supra*; nr. 531.

[1163] See also P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 133.

[1164] See also G. Hornung, "A General Data Protection Regulation for Europa? Light and Shade in the Commission's Draft of 25 January 2012", *Scripted 2012*, Volume 9, Issue 1, p. 70.

[1165] Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability", WP 173, 13 July 2010, p. 3. See also *infra*; nrs. 607 et seq.

[1166] G. Hornung, "A General Data Protection Regulation for Europa? Light and Shade in the Commission's Draft of 25 January 2012", *l.c.* p. 70. See also C. Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *l.c.*, p. 7 and P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143-144.

[1167] See article 35 of the Commission Proposal (Data Protection Officer).

processing before it is even initiated.[1168] Processors are also directly accountable towards supervisory authorities. For example, processors must (a) maintain and provide appropriate documentation upon request (article 28); (b) co-operate in case of an investigation (article 29) and (c) abide by administrative orders (article 53).[1169] In other words, the Commission proposal clearly affords the processor an "*independent position*" and a role "*which in some respects seems to equal that of the controller*".[1170]

546. REGULATING JOINT CONTROL – A third significant revision proposed by the Commission concerns the relationship between joint controllers. Article 24 essentially codifies the guidance issued by the Article 29 Working Party in Opinion 1/2010, by mandating that joint controllers determine their respective responsibilities for compliance by means of an "arrangement" between them, in particular as regards the procedures and mechanisms to accommodate data subject rights.[1171]

547. AMBIGUITY – The revisions proposed by the Commission regarding the obligations of controllers and processors were met with mixed reviews.[1172] Overall, it seems that the revised allocation of responsibilities proposed by the Commission did not resonate well with the traditional understanding of controller-processor relationships. Moreover, certain commentators felt that by imposing obligations directly on processors, there may be a risk of confusion as to who is ultimately responsible for ensuring compliance.[1173] For example, in relation to the data security obligation (article 30), the EDPS noted that:

[1168] See article 33 of the Commission Proposal (Data Protection Impact Assessment).

[1169] It is noteworthy that many processor obligations in the proposed Regulation appear to be directly applicable, as opposed to being dependent on a contract or legal act. At the same, the proposed Regulation still maintains the obligation for controllers to legally bind the processor to the same (and other obligations) by way of contract or other legal act in article 26(2).

[1170] P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143. Further indications of the independence of the processor include: the duty to have data protection officer (even in situations where the controller might not be obliged to have one (article 35); and the fact the legitimate interest of the processor may enable transfers which are neither frequent nor massive (Article 44(1h)). (*Ibid*, p. 144)

[1171] Compare *supra*; nr. 535.

[1172] See in particular European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", 7 March 2012, p. 31 (at paragraph 192); Information Commissioner's Office (ICO), "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper", v1.0, 12 February 2013, p. 9 en 35; P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 133-134; P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143-144; B. Treacy, "Challenging times ahead for data processors", *Privacy & Data Protection Journal* 2012 Vol. 12, Issue 7, p. 3-6; K. Irion and G. Luchetta, "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), April 2013, p. 46-48; Business Europe, "Commission Proposal on a General Data Protection Regulation", Position Paper, 17 October 2012, p. 11; European Banking Federation, "EBF Position on the European Commission's Proposal for a Regulation on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 22 May 2015, p. 9-10 and Association of Consumer Credit Information Suppliers (ACCIS), Position paper on proposed Data Protection Regulation, April 2012, p. 21.

[1173] See in particular P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143-144 and B. Treacy, "Challenging times ahead for data processors", *l.c.*, p. 5-6.

> "*In Article 30 on security of processing, reference is made to the controller and the processor. The EDPS welcomes that both actors are mentioned, but recommends the legislator to clarify the provision in such a way that there is no doubt about the overall responsibility of the controller. From the text as it currently stands, both the processor and the controller seem to be equally responsible. This is not in line with the preceding provisions, in particular Articles 22 and 26 of the proposed Regulation.*"[1174]

In the same vein, the ICO noted in relation to article 26 (processor) that

> "*[…] we need to be clear about who is responsible for what where a number of organisations are each involved in the processing of personal data, and, as drafted, this Article will not help us here.*"[1175]

Lack of dogmatic precision can also be found in the provision regarding processors who become joint controllers (article 26(4)).[1176]

548. LIABILITY – Article 77(2) of the Commission proposal provides that in case where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage. The imposition of joint and several liability was welcomed by both the Article

---

[1174] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", p. 31 (at paragraph 192). See also P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 144 ("*Article 30 is a problematic rule as the primary and determining responsibility should be placed solely at controller level […] There are naturally valid arguments for placing security obligations directly on the processor and against this background it is interesting and somewhat puzzling to notice that the obligations with respect to breach notification (Articles 31–32) rest exclusively on the controller. Security may be breached at many levels and there is no doubt that this will also occur at the processor level. As the processor in Article 30 is made independently responsible for security, it would seem logical that the processor should also report breaches; why this is not the case is uncertain.*")

[1175] Information Commissioner's Office (ICO), "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper", *l.c.*, p. 34. At the same time, the ICO also reiterated its earlier complaint regarding its difficulties to distinguish between controllers and processors in practice ("*It is fair to say that the ICO can find it difficult to determine which organisations are data controllers and which are processors. The problem arises because, given the collaborative nature of modern business, it is rare for a one organisation (the processor) to only act on instructions from another (the controller). There tends to be a considerable degree of freedom, skill, judgment and the like in terms of the way the first organisation provides services to the second, all against the backdrop of complex collaborative arrangements involving numerous organisations.*") (*Id.*)

[1176] See e.g. Information Commissioner's Office (ICO), "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper", *l.c.*, p. 35 ("*We can certainly see why a processor that takes a controller's data and then uses it for its own purposes should take on full data controller responsibility. However, this is different from failing to act on the data controller's instructions. We would have more difficulty with the idea that a processor becomes a controller because it has erased personal data by mistake, for example – this would amount to processing personal data other than as instructed by the data controller - but in a case like this the organisation should just be treated as a 'bad processor' rather than a data controller in its own right.*"). See also B. Treacy, "Challenging times ahead for data processors", *l.c.*, p. 4. In my view, the Commission proposal also errs by implicitly labelling a processor who re-purposes data as a "joint controller", as in the identified scenario the (former) processor does not determine the purposes and means "together with" the (initial) controller. Joint control suggests a joint determination of "purposes conditions and means" under article 24. (B. Treacy, "Challenging times ahead for data processors", *l.c.*, p. 6.) Compare also *supra*; nr. 114.

29 Working Party and the EDPS.[1177] The EDPS expressed concerns, however, that the provision could be interpreted as nevertheless requiring the data subject to choose between the controller and processor when seeking compensation:

> "*[Article 77] is reasonable and fair from the point of view of the data subject. He or she will usually not be able to do much more than alleging a breach and damage sustained from that breach. In contrast, controllers and processors have more access to the relevant facts of the event once they have been established.*
>
> *However, in view of the responsibility of the controller, a data subject should not have to choose between the controller and the processor. It should be possible always to address the controller, regardless of where and how the damage arose. The Regulation should provide for a subsequent settlement of the damages between the controller and the processor, once the distribution of liability among them has been clarified. The same applies to the case of multiple controllers and processors.*"[1178]

In my opinion, the imposition of joint and several liability in all cases "*where more than one controller or processor is involved in the processing*" is excessive. It would imply for example, that collaborating single controllers face joint and several liability even in cases where they do not make any joint determination regarding either the purposes and means of the processing.[1179] Under the literal wording of article 77(2), mere "involvement" – no matter how remote or indirect – would suffice to implicate an actor in a claim for damages.

B. First Reading European Parliament

549. PREFACE – On 16 February 2012, the European Parliament appointed its Committee on Civil Liberties, Justice and Home Affairs (LIBE) as the lead Committee to review the Commission's proposals.[1180] The LIBE Committee, with Jan Philipp Albrecht as its rapporteur, produced its first draft report on the proposed regulation on 16 January 2013.[1181] Following months of intense lobbying (which led to more than 3999

[1177] Article 29 Data Protection Working Party, "Opinion 01/2012 on the data protection reform proposals", WP 191, 23 March 2012, p. 23 and European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", *l.c.*, p. 44.

[1178] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", *l.c.*, p. 44.

[1179] Compare *supra*; nrs. 140 et seq.

[1180] See Legislative observatory, Procedure file 2012/0011(COD), accessible at http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29 (last accessed 15 October 2015).

[1181] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) 16 January 2013, accessible at

amendments in the LIBE committee alone[1182]), the LIBE committee produced a "comprise" text[1183] which would form the basis of its draft resolution.[1184] The official First Reading of the Parliament took place on 12 March 2014, when the Parliament almost unanimously adopted the resolution prepared by the LIBE Committee.[1185]

550. PRIOR ASSESSMENT – The LIBE Committee produced four "working documents" as part of its review of the data protection reform package. In its second Working Document, the Committee outlined its preliminary views regarding the distribution of responsibilities between controllers and processors contained in the Commission Proposal:

> *"The processing of personal data offers many business opportunities to data controllers and processors. However, since personal data protection is a fundamental right, this processing also entails responsibilities. These obligations should be clear and understandable to avoid legal uncertainty for companies and authorities, as well as for the data subjects. Therefore, a much clearer division of duties and responsibilities between data controllers and data processors is needed. More debate is needed on the concept of "joint controllers". Furthermore, we need a clarification on the limits of what a processor can do without being instructed by the controller, including when a processor enlists a sub-contractor for processing."*[1186]

---

http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.927 (last accessed 16 March 2015).

[1182] See J.P. Albrecht, "EU General Data Protection Regulation - State of play and 10 main issues", 7 January 2015, p. 1, accessible at https://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf (last accessed 15 October 2015).

[1183] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)) Compromise amendments on Articles 1-29, 7 October 2013, p. 4, accessible at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf.

[1184] Committee on Civil Liberties, Justice and Home Affairs, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), 21 November 2013, accessible at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN (last accessed 15 October 2015).

[1185] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), accessible at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212 (last accessed 15 October 2015).

[1186] European Parliament, LIBE Committee, "Working Document 2 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 8 October 2012, PE497.802v01-00, p. 5, accessible at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

The amendments which the LIBE Committee eventually proposed were influenced by the proposals made by the other Committees (ITRE, IMCO, JURI, EMPL), as well as continuous discussions with representatives of the Council, the Commission and other stakeholders.[1187] Prior to issuing its first Draft Report on the proposed Regulation in January 2013, the European Parliament's Directorate-General for Internal Policies published an external report (hereafter: "External Report").[1188] While the External Report did not contain any official viewpoint of the European Parliament, it served as an additional background document during the further deliberations. Where appropriate, reference will be made to the analysis contained in the External Report.

i. Definitions

551. OUTLINE – In its First Reading, the European Parliament proposed only one change regarding the concepts of controller and processor. Specifically, it proposed to delete the words "and conditions" from the definition of a controller. The definition of a processor remained unchanged. In other words, the European Parliament indirectly took the position that for both concepts the original definitions of Directive 95/46 should be maintained "as is".

552. DELETION OF "CONDITIONS" – The removal of "conditions" from the definition of a controller was supported by several Committee Opinions and amendments.[1189] The deletion of the term was also supported by the authors of the External Report, who argued that the addition of the term "conditions" was likely to cause more difficulties and uncertainties, rather than eliminate them.[1190]

%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-497.802%2b01%2bDOC%2bPDF%2bV0%2f%2fEN (last accessed 20 October 2015). An overview of the documentation produced by the European Parliament and its Committee can be found at http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20120514CDT45071#menuzone (last accessed 20 October 2015)

[1187] European Parliament, LIBE Committee, "Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 21 November 2013, A7-0402/2013, p. 199, accessible at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN. This report contains Opinions issued by the other Committees of The European Parliament (ITRE, IMCO, JURI, EMPL).

[1188] See X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", Study commissioned by the European Parliament, Directorate-General for Internal Policies, Policy Department A: Economic and Scientific Policy, IP/A/IMCO/ST/2012-02, PE 492.431, September 2012, at p. 33, accessible at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET%282012%29492431_EN.pdf (last accessed 8 February 2015).

[1189] See European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, Amendments 744-748). Several proposed amendments went even further, also deleting the word "means" from the definition, but these amendments were not retained by the LIBE Committee. Cf. *infra*; nr. 553.

[1190] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 30.

553. NO DELETION OF "MEANS" – Several Committee Opinions (ITRE, JURI and IMCO) and MEPs proposed to additionally remove the reference to "means" from the definition of a controller.[1191] The IMCO Opinion offered the following rationale for the change:

> *"With new technologies and services available such as cloud computing traditional division of entities involved in the processing of personal data may prove difficult, with the processor having in such cases significant influence over the way in which data are being processed. For this reason it seems reasonable to determine the controller as the entity, which decides over the purpose of processing personal data as determination of finality is the most important decision with the other factors serving as means to achieve it."*[1192]

The deletion of "means" was also supported by the authors of the External Report, who argued that abandoning the "means" criterion would be advisable because*:*

- *there are substantial doubts as how to understand the term "means";*
- *greater importance is already assigned to the factor of "determining the purposes" rather than "determining the means" of processing;*
- *Article 29 Working Party even permits the possibility of "delegation" of the competence to determine the means to the processor (at least as defined by the narrow meaning of that term);*
- *moreover, the general importance of "purposes" of processing is much higher in the personal data protection regulation because – as the legal literature reasonably notes – "the finality pursued by (a set of) processing operations fulfils a fundamental role in determining the scope of the controller's obligations, as well as when assessing the overall legitimacy and/or proportionality of the processing*".[1193]

[1191] See European Parliament, Opinion of the Committee on Industry, Research and Energy (ITRE), 26 February 2013, Amendment 80; Opinion of the Committee on Internal Market and Consumer Affairs (IMCO), 28 January 2013, Amendment 62; Opinion of the Committee on Legal Affairs (JURI), 25 March 2013, Amendment 38 and European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendments 746-48 .

[1192] European Parliament, Opinion of the Committee on Internal Market and Consumer Affairs (IMCO), 28 January 2013, amendment 62. In the same vein, MEP Adina-Ioana Vălean, Jens Rohde argued that "*The definition of controller should be based on the decision of the purposes for which personal data are processed rather than the conditions or means by which this is achieved. The control over the purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed.*" (European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendments 746). Other MEP's supported the change for a different reason, namely to clarify that only the controller and not the processor is responsible for compliance (See MEP amendments 748, with justification that: "*The aim of the change is not to lower the level of protection for the individual but to clarify that only the controller and not the processor is responsible. See related Amendments to articles 22, 24, 26 and 77.*")

[1193] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31, with reference to B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *Computer Law & Security Review* 2012, Vol. 28, p. 31, footnote 55.

The proposals to delete "means" were, however, received negatively by the European Data Protection Supervisor (EDPS). In particular, the EDPS considered that:

> "*Amendments related to controller/processor's roles appear in many parts of the text, including in the definitions. Several amendments would remove the notion that the controller determines not only the purposes but also 'the conditions and means' of the processing, as defined in Article 4(5) of the proposal (e.g. ITRE AM 81; IMCO AM 62; LIBE AM 746, 747, 748). The criteria that the controller determines the 'purposes and means' of the processing were set forth in Directive 95/46/EC and developed in the WP 29 Opinion 1/2010 on the concepts of 'controller' and 'processor'. These criteria have effectively contributed to the understanding and delineation of the roles of controllers and processors and should not be deleted.*"[1194]

554. KEEPING PROCESSORS – Following the initial proposal by the European Commission, De Hert and Papakonstantinou suggested that the time may have come to "boldly abolish" the concept of processor altogether.[1195] In this respect, the External Report mainly expressed caution.[1196] It argued that abolition of the controller and processor concepts would effectively render the positions of all actors involved in data processing "equal" and distribute all the obligations evenly "*without taking into account their individual position, the scope of their tasks, or the expectations of data subjects*".[1197] Moreover, it was argued that "*the removal of such an important class of entities from the regulation could result in a weakening of the level of data protection*".[1198] Finally, it was argued that one can – with proper interpretation – seemingly achieve results similar the ones envisaged by abandoning the processor concept.[1199] The External Report therefore concluded that further proposals should instead elaborate on a precise division and determination of the obligations and responsibilities of data controller and data processor.[1200] As indicated earlier, the LIBE Committee endorsed such an approach in its second Working Document on the general data protection regulation.[1201]

555. NO ADDITIONAL ACTORS – Finally, it is worth observing that the LIBE Committee also entertained proposals to introduce additional actors. In its first draft report, for

---

[1194] European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", 15 March 2013, p. 6 (at paragraph 24), accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf (last accessed 20 October 2015).
[1195] See e.g., P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 134.
[1196] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31.
[1197] *Id.*
[1198] *Ibid*, p. 32.
[1199] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31.
[1200] *Ibid*, p. 32.
[1201] Cf. *supra*; nr. 550.

example, the LIBE Committee proposed to introduce the concept of a "producer".[1202] It was argued that

> "*producers of automated data processing systems (i.e. hard- and software) should also take into account the principle of privacy by design and by default, even if they do not process personal data themselves. This is especially relevant for widely used standard applications, but also should be respected for niche products)*."[1203]

The proposed Amendment did not, however, make it to the First Reading. The same fate would await other proposals to introduce additional actors which were submitted by individual Members of Parliament.[1204]

ii. Obligations

556. OUTLINE – The First Reading introduced only minor changes to the distribution of responsibilities between controllers and processors. As in the initial Commission Proposal, the First Reading imposes a range of obligations *upon both controller and processor*, namely in relation to:

- the obligation to maintain documentation (article 28):
- co-operation with supervisory authorities (article 29):
- the obligation to maintain an appropriate level of data security (article 30)[1205];
- the obligation to notify data breaches (article 31)[1206];
- the obligation to conduct a risk analyses (article 32a) (new)[1207]:
- data protection impact assessments (article 33);
- data protection compliance reviews (article 33a) (new)[1208];

[1202] European Parliament, LIBE Committee, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD), PE501.927v04-00, 16 January 2013, p. 66 (Amendment 88), accessible at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0//EN&language=EN

[1203] *Ibid*, p. 71 (Amendment 98).

[1204] See European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendment 749-750 (proposing a distinction between "direct" and "indirect" controllers) and amendment 751 (proposing the concept of a "publisher").

[1205] The security obligations contained in article 30 were detailed further in the First Reading.

[1206] As regards the obligation to notify data breaches, a distinction should be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller (article 31(2)).

[1207] Article 32a requires both controller and processors to undertake a risk analysis relating to their processing activities in a catalogue of cases. The presence of one or more risks acts as a trigger for additional obligation outlined in article 32a(3) (appointing representative, designating DPO, conducting data protection impact assessment, consulting DPO or supervisory authority).

[1208] Article 33a requires the data controller or processor acting on the controller's behalf to carry out a periodic data protection compliance review.

- prior authorization (article 34);
- data protection officers (articles 35-37);
- codes of conduct (article 38);
- certification (article 39); and
- international transfers (articles 40-44).

One notable change concerns the requirement of *data protection by design and by default* (article 23), which under the First Reading also applies to processors.[1209] Still, the First Reading maintains that certain obligations should only apply to the controller. For example, the obligations to notify data breaches to supervisory authorities and data subjects (articles 31 and 32) still only apply to the controller.

557. RESPONSIBILITY OF THE CONTROLLER – Changes made to article 22 mainly served to enhance the emphasis on accountability. Not only was the word "accountability" added to the title of the article, several changes were made to expand the controller's obligation to *demonstrate* the adoption of measures to ensure compliance.[1210]

558. JOINT CONTROL – Article 24 underwent two significant changes. First, it was revised to provide a more precise and accurate description of the concept of "joint control".[1211] Second, the provision was extended to specify that the arrangement between joint controllers must

> "*duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable*."[1212]

[1209] While article 23(1) now also mentions processor, article 23(2) still only mentions controllers. Interestingly, the word "implement" in article 23(2) was replaced by "ensure", suggesting that the ultimate responsibility for the data protection impact assessment may have remained with the controller.

[1210] Articled 22(1) also adds a specific obligation to implement policies and procedures "*to persistently respect the autonomous choices of data subjects*". Article 22(2) of the Commission Proposal was removed in the First Reading, based on the consideration that it had no added value and failed to mention all obligations required by the Regulation. (See European Parliament, LIBE Committee, "Amendments 1493-1828", 6 March 2013, PE506.164v02-00, Amendment 1666). A similar outline of controller obligations was inserted in Recital (60).

[1211] Article 24 now refers to "*several controllers jointly determine purposes and means*" instead of "*a controller determines the purposes, conditions and means of the processing of personal data jointly with others*".

[1212] The first part of the revision to article 24 ("*the arrangement shall duly reflect …*") had been proposed by ITRE (321/623) and Am 1748 with following justification: "*The arrangement to be entered into by joint controllers should be expressly required to duly reflect the joint controllers' respective roles and relationships with the data subjects. Joint controllers are not necessarily in an equal negotiation position when it comes to contractual agreements. Moreover, not all joint controllers enjoy a direct relationship with the data subject and they do not control the same kind and amount of personal data.*"). The second party of the revision ("*in case of unclarity …*") was seemingly linked to the revisions made to article 77(2). Cf. *infra*; nr. 563.

559. CHOICE OF PROCESSOR – Article 26(1) did not undergo any revisions, save for the substitution of the words "a processing operation" with "processing" (presumably to ensure that the provision can be applied both at the level of an individual processing operation or set of processing operations).

560. LEGAL BINDING – Article 26(2) underwent substantial, albeit ambivalent, revisions. On the one hand, the provision was modified to recognize that controllers and processors should have flexibility in deciding how to allocate responsibilities among themselves. On the other hand, it also maintains that certain obligations should still be made applicable processors by way of a contract or other legal act.[1213] Specifically, article 26(2) provides that

> *"The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that the processor shall:*
>
> *(a) process personal data only on instructions from the controller, unless otherwise required by Union law or Member State law;*
>
> *(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality;*
>
> *(c) take all required measures pursuant to Article 30;*
>
> *(d) determine the conditions for enlisting another processor only with the prior permission of the controller, unless otherwise determined*
>
> *(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the appropriate and relevant technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*
>
> *(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34, taking into account the nature of processing and the information available to the processor;*
>
> *(g) return all results to the controller after the end of the processing, not process the personal data otherwise and delete existing copies unless Union or Member State law requires storage of the data;*

[1213] The ambivalence stems from the fact that the proposed revision in fact combines two different approaches. ITRE Amendment 223 sought to provide full flexibility in the distribution of roles and responsibilities (and to limit the number of obligations directly incumbent upon processors), whereas the text adopted in First Reading generally still renders processors directly responsible for complying with certain obligations. See also *infra*; nr. 568.

(h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow on-site inspections.[1214]

561. BOUND BY INSTRUCTIONS – No changes were made to article 27 in First reading. Article 26(4) was revised, however, to provide that:

> *"If a processor processes personal data other than as instructed by the controller or becomes the determining party in relation to the purposes and means of data processing, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24."*

The revision essentially further codified the guidance of the Article 29 Working Party Opinion 1/2010.[1215]

iii. Liability and sanctions

562. RIGHT TO COMPENSATION AND LIABILITY – Numerous proposals to amend article 77(1) were made prior to the First Reading. Certain amendments sought to remove liability of processors (e.g., amendments 2818, 2822 and 2825), or to make processor liability contingent upon a disregard of the instructions issued by the controller (amendment 2823). Another proposal sought to exempt both controllers and processors from liability in case of damages caused by unintentional and non-negligent behaviour (amendment 2819).[1216] In the end, the changes to article 77(1) were relatively minor. The First Reading only substituted the wording "right to receive from" with the words "claim from" and clarified that the right to compensation extends to "non-pecuniary damages".

563. JOINT AND SEVERAL LIABILITY – A more significant change was made to article 77(2), which was revised to make joint and several liability conditional upon absence of an "appropriate written agreement". Specifically, revised article 77(2) provided that

> "*Where more than one controller or processor is involved in the processing, each of those controllers or processors shall be jointly and severally liable for the entire amount of the damage, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24.*"

[1214] The removal of the reference to "and supervisory authorities" in article 26(2)h was simply motivated by the fact that the powers of supervisory authorities are dealt elsewhere See European Parliament, LIBE Committee, "Amendments 1493-1828", 6 March 2013, PE506.164v02-00, Amendment 1801).

[1215] The revision failed, however, to accommodate the commentary by the Information Commissioner's Office (ICO) regarding the distinction between processors who re-use personal data for a new purpose and processors who simply fail to give effect to certain instructions ("bad" processors). Cf. *supra*; footnote 1176.

[1216] See European Parliament, LIBE Committee, Amendments 2618 – 2950, 6 March 2013, PE501.927v04-00, amendments 2818-2825.

The revision essentially consisted of a further codification of the guidance issued by the Article 29 Working Party in 1/2010.[1217] Oddly, article 24 only referred to *joint controllers* (whereas article 77(2) imposes solidary liability on both controllers and processors who are "involved" in the processing).[1218]

564. EXEMPTIONS – The liability exemption of article 77(3) was not modified in the First Reading. Likewise, article 3(3) still incorporated the intermediary liability exemptions contained in the e-Commerce Directive.[1219]

565. PENALTIES – Article 78 was not modified in First Reading.

566. ADMINISTRATIVE SANCTIONS – Article 79 underwent substantive revisions in First Reading, but the revisions did not affect the existing premise that administrative sanctions can be imposed "anyone who" fails to comply with the relevant provisions.[1220]

iv. Assessment

567. BACK TO SQUARE ONE – The First Reading made a full return to the definitions of Directive 95/46. The term "conditions" was deleted from the definition of a controller. Despite support by several MEPs to also delete the reference to "means", the LIBE Committee decided to keep controller "as is". This was seemingly born out of the recognition that common understanding of both the controller concepts cannot be disassociated from the existing criteria.[1221] Proposals to introduce additional actors were not accepted. The First Reading thus continued in the same vein as the initial Commission Proposal, leaving existing concepts intact.

[1217] This rationale is explicitly confirmed by the justification accompanying amendment 2827 ("*Creates an incentive for clarifying the roles and responsibilities in writing in cases where several controllers or processors are involved, in line with Art. 29 Working Party, Opinion 169.*") Likeminded revisions were proposed by way of amendments 2826, 2828-2830. See European Parliament, LIBE Committee, Amendments 2618 – 2950, 6 March 2013, PE501.927v04-00, amendments 2826-2830.

[1218] Several proposals were made to delete 24(2) in its entirety (see amendments 2832-2833), but none of these amendments were retained. See European Parliament, LIBE Committee, Amendments 2618 – 2950, 6 March 2013, PE501.927v04-00, amendments 2826-2830.

[1219] It is worth noting that in its first draft report, the LIBE Committee seemed inclined to reverse the approach taken by the European Commission, but in the end left it the way it was. See European Parliament, LIBE Committee, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) 16 January 2013, p. 13, accessible at http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.927 (last accessed 20 October 2015).

[1220] Article 79(2) still provides, however, that the "degree of responsibility" of the natural or legal person shall be taken into account when determining the amount of an administrative fine.

[1221] See also European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", 15 March 2013, p. 5 (at paragraph 24), accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

568. PROCESSOR OBLIGATIONS – Overall, the First Reading proposed only minor changes to the distribution of responsibilities between controllers and processor. Despite several proposals to remove or limit the obligations of processors, the First Reading retained the approach that certain obligations should be directly incumbent upon processors.[1222] In this regard, the LIBE Committee may have felt supported by the additional comments provided by the European Data Protection Supervisor:

> *"Many amendments aim at diminishing the responsibility of the processor foreseen in the proposal, for example by removing or weakening the obligations that the processor maintains documentation, carries out a data protection impact assessment (DPIA), or helps the controller comply with security requirements (i.e. ITRE AM 43, 229, 233, 238, 260; LIBE AM 1829, 1832, 1834, 1836, 1837, 2024). However, the extension of certain obligations to processors reflects the current growing role of processors in determining certain essential conditions of the processing (e.g. in the context of cloud computing, where they often decide on transfers and sub- processing). In this context, processors should also be accountable for their processing."*[1223]

569. FURTHER CODIFICATION OF OPINION 1/2010 – Several amendments which were incorporated in the First Reading can be seen as attempts to further codify the guidance issued by the Working Party in Opinion 1/2010. Clear examples are the amendments proposed to article 26(4) (processor becomes controller if he processes personal data other than as instructed by the controller or becomes "the determining party" in relation to the purposes and means of data processing) and article 77(2) (making joint and several liability of joint controllers conditional upon the absence of an arrangement appropriately allocating responsibilities).

570. AMBIGUITY REMAINS – The First Reading still contains traces of ambivalence with regards to the role of the processor (e.g., in article 26(2)) as well as a lack of dogmatic precision in several provisions (e.g., the discrepancy between article 24 and article 77). It also failed to resolve the basic concerns previously articulated regarding the lack of clarity in the nature of the distribution of responsibilities between controllers and processors.

[1222] In fact, an additional processor obligation: article 31(1) (data protection by design) was also made applicable to processors under the First Reading.

[1223] European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", *l.c.*, p. 6 (at paragraph 25).

C. *General Approach of the Council*

571. PREFACE – The Council's approach to adopting a "common position" was an incremental one. Discussions at the level of the Council of the European Union began as early as March of 2012.[1224] The review of the GDPR at the level of the Council was handled by the Working Party on Information Exchange and Data Protection (DAPIX), which conducted a series of article-by-article and chapter-by-chapter discussions, under the auspices of various presidencies.[1225] The European Council finally reached consensus on a General Approach to the GDPR under the Luxembourg Presidency on 15 June 2015, more than three years after discussions had been initiated.[1226]

i. Definitions

572. IDENTICAL TO FIRST READING – Like the European Parliament, the Council rejected the Commission's proposal to add a reference to "conditions" to the definition of controller. The General Approach thus also returned to the 1995 definitions of controller and processor.

ii. Obligations

573. OUTLINE – The General Approach introduced significant changes to the distribution of responsibilities between controllers and processors. Several provisions remained relevant to *both controller and processor*, in particular:

- the obligation to maintain documentation (article 28)[1227]
- co-operation with supervisory authorities (article 53 et seq.);
- the obligation to maintain an appropriate level of data security (article 30);
- the obligation to notify data breaches (article 31)[1228];

[1224] See Council of the European Union, Working Party on Information Exchange and Data Protection (DAPIX), "Outcome of proceedings – summary of discussions on 23-24 February 2012", 8 March 2012, 2012/0011 (COD), 7221/12, DAPIX 22, accessible at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207221%202012%20INIT.

[1225] Discussion in the DAPIX Council began in March 2012 under the Danish Presidency. Subsequent presidencies were held by Cyprus, Ireland, Lithuania, Greece, Italy, Latvia and Luxembourg. For an overview of the documents adopted under each presidency see https://www.wsgr.com/eudataregulation/process-updates.htm.

[1226] Council of the European Union (Press release), "Data Protection: Council agrees on a general approach", 15 June 2015, accessible at http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection and Council for the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 11 June 2015, 2012/0011 (COD), 9565/15, accessible at http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf (last accessed 21 October 2015).

[1227] While the both controllers and processors are obliged to maintain certain documentation, article 28 distinguishes between both actors in terms of the types of documentation they must maintain.

- data protection officers (articles 35-37);
- codes of conduct (article 38);
- certification (article 39); and
- international transfers (articles 40-44).

An increased number of obligations, however, were rendered *applicable only to controllers*, in particular:

- compliance (and demonstration of compliance) with principles relating to the processing of personal data (article 5).
- data protection by design and by default (article 23)[1229];
- notification of data breaches to supervisory authorities and data subjects (article 31-32)[1230];
- data protection impact assessment (article 33)[1231]; and
- prior consultation (article 34)[1232].

574. RESPONSIBILTY OF THE CONTROLLER – Article 22 was revised, primarily to reflect "*a more risk-based*" approach. The Council members generally felt that such an approach was necessary to reduce administrative burden and compliance costs.[1233] As a result, article 22 was revised to make clear that the controller's obligation to adopt "appropriate measures" shall be determined inter alia on the basis of the "*likelihood and severity*" of the risks presented by the processing.[1234] Similar references to risk considerations were inserted in articles 30-34.

575. JOINT CONTROL – Article 24 was extended to further elaborate upon the key elements of the mandatory "arrangement" between joint controllers. The arrangement

---

[1228] As regards the obligation to notify data breaches, a distinction should be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller (article 31(2)).
[1229] In its First Reading, the European Parliament proposed to extend article 23 to processors.
[1230] As in the Commission Proposal and the First Reading of the Parliament, the obligation to notify the supervisory authority and data subject was exclusively incumbent upon controller. The processor, however, was still under an obligation to notify the controller in case of breach (article 31(2)).
[1231] Contrary to Commission Proposal and First Reading.
[1232] Contrary to Commission Proposal and First Reading.
[1233] See e.g. "Press Release - 3207th Council meeting - Justice and Home Affairs Brussels - 6 and 7 December 2012", 17315/12 PRESSE 509 PR CO 70, p. 13; Council of the European Union, Note from the Presidency to the Council regarding the General Data Protection Regulation – implementation of risk-based approach – Flexibility for the Public Sector, 2012/0011 (COD), 6607/1/13 REV 1, 1 March 2013, p. 2-4; Council of the European Union, Note from the Presidency to the Working Party on Information Exchange and Data Protection regarding the General Data Protection Regulation – risk-based approach, 2012/0011 (COD), 11481/14, 3 July 2014, p. 1-5.
[1234] While the European Parliament in its First Reading also added reference to risks, it did not include the terms "likelihood and severity".

should cover the information obligations of controllers as well as provide for "single point of contact" for the exercise of data subject rights.[1235]

576. LEGAL BINDING – Like article 24, article 26(2) was extended to further elaborate upon the key elements to be included in the arrangement between controllers and processors. In particular, a greater emphasis was placed on addressing subprocessing (see e.g. article 26(2)a) and the use of standardised contracts.

577. BOUND BY INSTRUCTIONS – The General Approach deleted both article 26(4) and article 27 entirely. The requirement to obtain permission from the controller for subprocessing was dealt with in article 26(2), whereas the consequences of a disregard for instructions was dealt with in article 77(2).

iii. Liability and sanctions

578. RIGHT TO COMPENSATION AND LIABILITY – The issue of liability of controllers and processors was discussed extensively by DAPIX.[1236] In the end, article 77(1) retained the general principle that individuals suffering damages as a result of unlawful processing should be able to receive compensation from the controller or processor. However, article 77(2) was revised to *differentiate* between the respective liability exposure of each actor:

> *"Any controller (…) involved in the processing shall be liable for the damage caused by the processing which is not in compliance with this Regulation. A processor shall be liable for (…) the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller."*

The change intended to clarify that a controller should in principle be liable for *any* damages arising from the unlawful processing personal data; whereas a processor would in principle only be liable "*for his segment*". [1237] As a result, the processor would

---

[1235] Pursuant to article 24(2), the data subject would still be able to exercise his or her rights against each of the joint controllers, irrespective of the designation of a single point of contact (unless the data subject was clearly informed of the respective responsibilities of each controller and the arrangement of the respective joint controllers clearly communicated to data subjects in transparent way and said arrangement is not "unfair" with regard to his or her rights - article 24(3)).

[1236] See e.g. Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection on the proposed General Data Protection Regulation – Chapter IV, 2012/0011 (COD), 12312/14, 1 August 2014, p. 5 and the DAPIX deliberations regarding Chapter VIII cited in the footnotes that follow.

[1237] See Council of the European Union, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 2012/0011 (COD), 7586/1/15 REV 1, 10 April 2015, in particular at p. 11 (Germany); 23-24 (France); p. 27 (Croatia) and 63 (Portugal). See also Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 9083/15, 27 May 2015, p. 2 (""*As most of the obligations in the Regulation, in particular in Chapter IV, rest with controllers, in many cases the controllers will be primarily liable for damages suffered as a consequence of data protection violations. However, a data subject which has suffered damages due to unlawful processing should also have the possibility to sue directly the processor in case he knows or has strong reasons to believe the processor and*

face liability only in case of failure to comply with those obligations of the Regulation which are specifically directly to him or if he acted contrary to or outside of the lawful instructions of the controller.[1238]

579. EXEMPTIONS – Article 77(3) was extended to clarify the exemptions shall only be relevant once liability has been established

> *"A controller or the processor shall be exempted from liability <u>in accordance with paragraph 2</u>, (…) if (…) it proves that it is not in any way responsible (…), for the event giving rise to the damage."*

Article 2(3) of the Commission Proposal, which contained a reference to the liability exemptions contained in the e-Commerce Directive, was deleted. Recital (17) still provided, however that:

> "*This Regulation should […] be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.*"

580. "CUMULATIVE" LIABILITY – Because several DAPIX delegations disliked the term "joint and several" liability, the decision was made to drop the terms entirely.[1239] Instead, article 77(4) would specify in which cases a controller or processor involved in the processing might be held liable "*for the entire damage*":

> *"Where more than one controller or processor or a controller and a processor are involved in the same processing <u>and, where they are, in accordance with paragraphs 2 and 3, responsible for any damage caused by the processing</u>, (…) each controller or processor shall be held (…) liable for the entire damage."*

The proposed revisions to article 77(4) significantly limited the instances in which a controller or processor might face cumulative liability. The liability of either controller or processor for the entire damage was made conditional upon a prior finding of responsibility in causing the damage.[1240] Only in cases where the controller or processor could be deemed responsible in accordance with paragraphs 2 and 3 could either of them be held liable for the entire damage.[1241]

<u>not (only) the controller is in fact liable</u>. Paragraph 1 clearly acknowledges that and leaves any person the choice to sue the controller, the processor or both. The controller can thus be the so-called single point of entry, but the data subject may choose another procedural avenue.")

[1238] *Id.*

[1239] Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p. 3 ("*Given the fact that the concept of joint and several liability seems to mean different things to different delegations, the new drafting avoids this term altogether.*")

[1240] See Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p 3.

[1241] Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p 3 ("*[E]ach non-compliant controller and/or processor involved in the processing are held liable for the entire amount of the damage. However a controller or processor is exempted from this liability if it demonstrates that it is not*

581. JOINED PROCEEDINGS – Recital (118) of the General approach clarified that in case of joined proceedings, compensation may be apportioned among the controller and processor who are liable according to their responsibility for the damage caused.[1242] Specifically, recital (118) provided that

> "*Where controllers or processors are involved in the same processing each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with national law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor who has (…) paid full compensation, may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.*"

582. RECOURSE – A new paragraph was added to article 77 to clarify that, in the absence of joined proceedings, a controller or processor who has been held liable "for the entire damage" is entitled to obtain redress from the other actors involved in the processing (insofar as they are may also be deemed responsible the damage). Specifically, article 77(5) of the General Approach provided that

> "*Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2.*"

583. ADMINISTRATIVE FINES – Under the General approach, a supervisory authority can in principle impose fines upon either controller or processor (article 79a).[1243] Such fines should be effective, proportionate and dissuasive penalties.

584. PENALTIES – Article 78 was deleted. A new article 79b was introduced to cover infringements which are not subject to administrative fines pursuant to article 79a (e.g., violations of Chapter IX – specific data processing situations), calling on Member States to introduce effective, proportionate and dissuasive penalties.

---

responsible for the damage (0% responsibility). Thus only controllers or processors that are at least partially responsible for non-compliance (however minor, e.g. 5%) with the Regulation, and/or in case of a processor, with the lawful instructions from the controller, can be held liable for the full amount of the damage.")

[1242] See also the introductory notes by the Presidency accompanying the General Approach: Council for the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 11 June 2015, 2012/0011 (COD), 9565/15, p. 2-3.

[1243] Article 79a(1) only mentions the controller, but the remaining provisions indicate that both controller and processor might be fined.

iv. Assessment

585. SIGNIFICANT CHANGES – While the General Approach left the 1995 concepts of controller and processor intact, it introduced significant changes to the distribution of responsibility and liability between controllers and processors. In comparison to the initial Commission Proposal, the General approach (a) imposed less obligations directly upon processor and (b) limited the instances in which controllers or processors might be held liable "for the entire damage".

586. LESS OBLIGATIONS FOR PROCESSORS – During their deliberations, the delegates to the DAPIX Working Party frequently expressed their concerns regarding the lack of clarity in the distribution of responsibilities between controllers and processors.[1244] Many expressed the view that the controller should continue to face "primary" responsibility for compliance.[1245] The obligations incumbent upon processors therefore needed to be limited, as did the corresponding liability exposure.[1246] Although the General Approach did not fully return to 1995 situation (in which processors are in principle only indirectly accountable), it imposed fewer obligations on processors in comparison to the Parliament's First Reading and the initial Commission proposal.[1247]

587. LESS CUMULATIVE LIABILITY – The issue of cumulative[1248] liability was discussed at length in the DAPIX Working Party.[1249] During the deliberations, the UK

[1244] See e.g. Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) – Specific Issues of Chapters I-IV of the General Data Protection Regulation – certain aspects of the relationship between controllers and processors, 2012/0011 (COD), 5345/14, 15 January 2014. Cloud computing was cited as a particular area of concern.

[1245] See e.g. Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) on the General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 7722/15, 13 April 2015, p. 2.

[1246] Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) on the General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 7722/15, 13 April 2015, p. 2-3.

[1247] For example, in the initial Commission proposal the obligation to conduct data protection impact assessments or to undertake prior consultation (article 33-34) were also relevant to processors.

[1248] As indicated earlier, the DAPIX Working Group decided to remove the term "joint and several liability" from the text because the concept meant different things to different delegates.

[1249] See in particular Council of the European Union, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 2012/0011 (COD), 7586/1/15 REV 1, 10 April 2015, p. 73-76 (UK arguing strongly in favor of "liability follows fault"); Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) on the General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), p. 3-4 (outlining 3 possible options); Council of the European Union, Note from the German delegation to the Working Group on Information Exchange and Data Protection (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/15, 21 April 2015 (Germany seeking to still retain joint and several liability, but to limit to specific instances); Council for the European Union, Note from the Presidency to the JHA Counsellors DAPIX on a Proposal for a General Data Protection Regulation – Chapter VIII, 8371/15, 4 May 2015; Council of the European Union, Note from the German delegation to the JHA Counsellors (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/1/15, 6 May 2015 (Germany updates its proposals); Council of the European Union, Note from the Presidency to the Permanent Representatives Committee on the proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8383/15, 13 May 2015 and

delegation argued heavily in favour of a system of "liability follows fault".[1250] In its view, general imposition of joint and several liability regardless of fault (as provided by the Commission Proposal) would have several disadvantages.[1251] Other delegations, the German delegation in particular, sought to retain the principle of joint and several liability, but agreed that it should be limited to instances the controller or processor were liable to the same damage pursuant article 77(1).[1252] Based on the discussions, the Latvian Presidency was able to narrow the choice down to two options.[1253] Under option 1, each controller and/or processor involved in the processing could be held liable for the entire amount of the damage, provided a shortcoming had been established.[1254] Under option 2, each controller involved in the processing could theoretically be held liable, regardless of fault.[1255] The first option was considered fairer towards the actors involved in the processing, as no actor faced liability if it bore no responsibility at all for the damage.[1256] The second option was considered to be more friendly towards the data subject, but excessive (in particular from the point of view of SME's).[1257] In the end, the choice was made for option 1.

588. CONSISTENCY WITH PETL – The Council's General Approach regarding "cumulative" liability reflects the general principles of tort law regarding multiple tortfeasors. According to article 9:101 of the Principles of European Tort Law (PETL), liability is solidary "*where the whole or a distinct part of the damage suffered by the victim is attributable to two or more persons*".[1258] The same provision also stipulates that where persons are subject to solidary liability, the victim may claim full compensation from any one or more of them, provided that the victim may not recover more than the full amount of the damage suffered by him.[1259] The main innovation of the General Approach in comparison to Directive 95/46 therefore does not relate to the imposition of "cumulative" or solidary liability (as the General Approach merely clarifies general tort law principles), but rather to the fact that the General Approach also imposes

---

Council of the European Union, Note from the Presidency to JHA Counsellor DAPIX on the Proposal for General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015.

[1250] Council of the European Union, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 2012/0011 (COD), 7586/1/15 REV 1, 10 April 2015, p. 73-76.

[1251] *Ibid*, p. 74.

[1252] See Council of the European Union, Note from the German delegation to the Working Group on Information Exchange and Data Protection (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/15, 21 April 2015 and Council of the European Union, Note from the German delegation to the JHA Counsellors (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/1/15, 6 May 2015.

[1253] Council of the European Union, Note from the Presidency to JHA Counsellor DAPIX on the Proposal for General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p. 3-4.

[1254] *Ibid*, p. 3

[1255] *Ibid*, p. 19.

[1256] *Id.*

[1257] *Ibid*, p. 4

[1258] See also *supra*; nr. 146.

[1259] See also *supra*; nr. 138.

obligations directly upon processors (albeit less extensively than either the initial Commission proposal or Parliament's First Reading).

D. Trilogue and final text

589. PREFACE – The trilogue negotiations between the European Commission, Council and Parliament were launched following the Council's adoption of the General Approach. A political agreement among the three bodies was achieved six months later, on 15 December 2015.[1260] The text resulting from the trilogue was made publically available on 28 January 2016.[1261] After making a number of linguistic and numbering edits, the Council adopted its First Reading of the GDPR on 6 April 2016.[1262] The European Commission expressed its support for the Council position at First reading on 11 April 2016.[1263] On 14 April 2016, the European Parliament approved the Council position at first reading, thereby concluding the legislative process.[1264] On 4 May 2016, the final text of GDPR was published in the Official Journal of the European Union.[1265]

[1260] European Commission, Agreement on Commission's EU data protection reform will boost Digital Single Market, Press Release, Brussels, 15 December 2015, available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm (last accessed 31 March 2016).

[1261] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Political agreement", 5455/16, 28 January 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN (last accessed 7 April 2016).

[1262] Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 5419/16, 6 April 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN (last accessed 7 April 2016).

[1263] European Commission, Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, COM(2016) 214 final, 11 April 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016PC0214&from=EN (last accessed 12 April 2016).

[1264] European Parliament, "Data protection reform - Parliament approves new rules fit for the digital era", Press Release, 14 April 2016, available at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20160407IPR21776/20160407IPR21776_en.pdf. See also European Commission, "Joint Statement on the final adoption of the new EU rules for personal data protection", 14 April 2016, available at http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (last accessed 14 April 2016).

[1265] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* 4 May 2016, L 119/1.

i. Definitions

590. IDENTICAL TO DIRECTIVE 95/46 – The GDPR replicates the definitions of controller and processor as defined by Directive 95/46. Only minor linguistic edits were made. Article 4 of provides that

> "(7) *'controller' means the natural or legal person, public authority, agency or ~~any~~ other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of <u>such</u> processing are determined <u>by Union or Member State law</u>, the controller or the specific criteria for ~~his~~ <u>its</u> nomination may be ~~designated~~ <u>provided for by Union or Member State law</u>;*"
>
> *(8) 'processor' means a natural or legal person, public authority, agency or ~~any~~ other body which processes personal data on behalf of the controller.*"

ii. Obligations

591. OUTLINE – The GDPR contains the same distribution of responsibilities between controllers and processors as the General Approach of the Council. The following provisions are relevant to *both controller and processor*:

- the obligation to maintain records of the processing (article 30);
- co-operation with supervisory authorities (article 58 et seq.);
- the obligation to notify data breaches (article 33)[1266];
- the obligation to maintain an appropriate level of data security (article 32);
- data protection officers (articles 37-39);
- codes of conduct (article 40);
- certification (article 42); and
- international transfers (articles 44-49).

The following obligations apply directly *only to controllers*:

- compliance (and demonstration of compliance) with principles relating to the processing of personal data (article 5);
- data protection by design and by default (article 25);
- notification of data breaches to supervisory authorities and data subjects (article 33-34);
- data protection impact assessment (article 35); and

[1266] As regards the obligation to notify data breaches, a distinction should be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller (article 31(2)).

- prior consultation (article 36).

592. RESPONSIBILTY OF THE CONTROLLER – Article 24 of the GDPR provides that

> "*1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*
>
> *2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.*
>
> *3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.*"

In comparison to the General Approach, article 24 was extended to recognise that the likelihood and severity of risks may vary. It now also states explicitly that measures to address risks must be reviewed and updated where necessary.

593. JOINT CONTROL – Article 26 of the GDPR provides that

> "*1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.*
>
> *2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.*
>
> *3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.*"

A noteworthy change to article 26(1) *in fine*, in comparison to the General Approach, lies in the fact that the designation of a point of contact for data subjects in the arrangement between joint controllers is no longer mandatory (the word "shall" was substituted with the word "may"). A second noteworthy change is that article 26(3) no longer provides

for an exception to the rule that a data subject may exercise his or her rights against each of the joint controllers involved in the processing.

594. CHOICE OF PROCESSOR – Article 28(1) of the GDPR provides that

"*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*"

595. LEGAL BINDING – Article 28(3) of the GDPR provides that

"*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and

deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions."

In case of sub-processing, the same data protection obligations as set out in the contract or other legal act between the controller and the processor must be imposed on that other processor by way of a contract or other legal act under Union or Member State law. Should the sub-processor fail to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations (article 28(4) of the GDPR).

The only notable change to article 28(3) GDPR, in comparison to the General Approach, is the addition of lit b), which requires the stipulation that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

596. BOUND BY INSTRUCTIONS – Article 29 of the GDPR provides that

"*The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.*"

In addition, article 28(10) of the GDPR provides that if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing (without prejudice to articles 82, 83 and 84).

iii. Liability and sanctions

597. RIGHT TO COMPENSATION AND LIABILITY – Article 82 of the GDPR provides that

"*1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of

this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

598. EXEMPTIONS – Article 82(3) of the GDPR provides that

"*A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.*"

In addition, article 2(4) of the GDPR provides that

"*This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.*"

599. CUMULATIVE LIABILITY – Article 82(4) of the GDPR provides that

"*Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.*"

600. JOINED PROCEEDINGS – Recital (146) of the GDPR provides that

"*Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.*"

601. RECOURSE – Article 82(5) of the GDPR provides that

"*Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.*"

602. ADMINISTRATIVE FINES –Article 83 of the GDPR provides that

"1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred

to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

603. PENALTIES – Article 84(1) of the GDPR provides that

"*Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.*"

iv. Assessment

604. MINOR CHANGES – In comparison to the General Approach of the Council, the changes introduced in the final text of the GDPR were relatively minor. While the concepts of controller and processor underwent linguistic edits, these edits in no way modified the content of the definitions. The provision on joint control was modified to stipulate that the designation of a single point of contact is not mandatory in all instances. It also removed the exception which provided that the data subject might not be able to exercise his rights against every joint controller in cases where "*the data subject has been informed in a transparent and unequivocal manner which of the joint controllers is responsible*". The reference to the liability exemptions contained in articles 12-15 of the E-Commerce Directive was reinstated in the body of the text, otherwise no substantive changes were made to the provisions concerning liability.[1267]

2.2 CONCLUSION

605. OUTLINE – The GDPR left the concepts of controller and processor intact. Only minor linguistic edits were made to the definitions contained in Directive 95/46. The GDPR did, however, introduce substantial changes as regards the allocation of responsibility and risk between controllers and processors. In comparison to Directive 95/46, the GDPR

(a) increased the emphasis on controller accountability;

(b) increased the number of obligations directly applicable processors and rendered them liable towards data subjects;

(c) explicitly addressed the relationship between joint controllers; and

(d) introduced a "cumulative" liability regime.

A. Controller accountability

606. BACKGROUND – The GDPR specifies in considerable detail the measures which controllers are expected to put in place in order to ensure compliance. Many of the measures required under Chapter IV of the GDPR can be traced back to policy debates surrounding the principle of "accountability".[1268] From 2009 onwards, data protection

[1267] Perhaps an important clarification was introduced in article 28(10) which specified that if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall not only be considered to be a controller in respect of that processing, but may also be held liable under articles 82 ,83 and 84.

[1268] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, *l.c.*, p. 10. See also the Revised OECD Privacy Guidelines, which introduced a new part entitled "implementing accountability" (Part Three), which outlined measures similar in nature.

authorities regularly met with industry representatives and other stakeholders to explore the potential of accountability as a means to address compliance challenges posed by emerging technologies and business models.[1269] The main purpose of these meetings was to determine whether or not the representatives from the various stakeholder groups could reach a consensus position on what it meant for an organisation to be "accountable" and what frameworks of compliance might be.[1270]

607. PRINCIPLE – Accountability is a concept with many dimensions.[1271] It has been characterized by scholars as being an "elusive" and even "chameleon-like" concept, because it can mean very different things to different people.[1272] In its core meaning, accountability refers to the existence of a relationship whereby one entity has the ability to call upon another entity and demand an explanation and/or justification for its conduct.[1273] Over time, different data protection instruments have advanced different types of accountability mechanisms.[1274] In the GDPR, the principle of accountability is mainly used to signal that controllers are not only *responsible* for implementing appropriate measures to comply with the GDPR, but must also be able to *demonstrate* compliance at the request of supervisory authorities.[1275]

[1269] J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 59.

[1270] *Id.* The Center for Information Policy Leadership (CIPL) acted as a driving force behind many of these meetings. Many of the discussion papers, which in first instance focused on elaborating the "essential elements" of accountability can be accessed at https://www.informationpolicycentre.com/resources/#accountability (last accessed 12 April 2016). In 2010, the Article 29 Working Party issued its own opinion on the principle of accountability (Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability", 13 July 2010, WP173). Already in 2009, however, the Working Party recommended that the Commission to consider "accountability-based mechanisms" and the introduction of an accountability principle in the revised Data Protection Directive in its Opinion on the Future of Privacy (W168, December 2009, paragraph 79).

[1271] See e.g. J. Koppell, "Pathologies of Accountability: ICANN and the Challenge of "Multiple accountabilities Disorder"", *Public Administration Review* 2005, vol. 65, p. 94-99 and R. Mulgan, ""Accountability": an ever-expanding concept?", *Public Administration* 2000, vol. 78 p. 555-556.

[1272] A. Sinclair, "The Chameleon of Accountability: Forms and Discourses", *Accounting, Organisations and Society* 1995, Vol. 20, p. 219 and M. Bovens, "Analysing and Assessing Accountability: A conceptual Framework", *European Law Journal* 2007, vol. 13, p. 448.

[1273] J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 71.

[1274] *Id.* The principle of accountability made its formal debut in the field of international data protection in the 1980 OECD Privacy Guidelines. For a discussion of the role of the accountability principle in different data protection instruments see J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 52-64. When reviewing these instruments, it is apparent where these instruments purport to rely on the same principle of accountability, notable differences exist in terms of the definition of norms, the designation of accountors and accountees, oversight mechanisms and sanctions. (*Id.*)

[1275] Article 5(2) of the GDPR specifies that the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to the processing of personal data. In the same vein article 24(1) provides that the controller shall *implement* appropriate technical and organisational measures to ensure and to be able to *demonstrate* that processing is performed in accordance with this Regulation. See also Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability", 13 July 2010, WP 173, paragraph 34. In the same vein, paragraph 15 of the Revised OECD Privacy Guidelines provide that a controller should put in place a privacy management programme which "gives effect" to the Guidelines for all personal data under its control, and should be prepared to

608. IMPLEMENTING ACCOUNTABILITY – Article 24(1) of the GDPR confirms that the controller is obliged to implement appropriate technical and organisational measures to ensure compliance. Generally speaking, this will require controllers to put in place internal policies and procedures dedicated to ensure organisational compliance (article 24(2)). The actual measures adopted by controllers must be tailored to the nature, scope, context and purposes of the processing, as well as the risks presented by the processing.[1276] Beyond these general statements of principle, the GDPR also specifies a number of specific obligations which aim to give further substance to the accountability principle, such as obligations concerning:

(a) data protection by design and by default (article 25)[1277]

(b) the legal binding of processors (article 28(3))[1278];

(c) the keeping of appropriate records of the processing (article 30)[1279];

(d) co-operation with supervisory authorities (article 31);

(e) personal data breach notification (article 33-34);

(f) data protection impact assessments and prior consultation (article 35-36);

(g) designation of data protection officer (article 37-39); and

(h) codes of conduct and certification (article 40-43).

B. Enhanced obligations for processors

609. MAIN OBLIGATIONS – In contrast to Directive 95/46, the GDPR contains a substantial number of provisions which are directly relevant to processors. Whereas processors were in principle only indirectly accountable under Directive 95/46, the GDPR imposes a range of obligations upon processors and renders them liable towards data subjects in case of non-compliance. Processors are also accountable to regulators, and can be fined in case of non-compliance with the obligations of the GDPR which are relevant to them. The following table provides a comparative overview of provisions

---

demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority.

[1276] Article 24(1) GDPR; Recital (74) GDPR. See also Paragraph 15(a)ii of the Revised OECD Privacy Guidelines (which provides that every controller should have in place a privacy management programme that is tailored "to the structure, scale, volume and sensitivity of its operations" and "provides for appropriate safeguards based on privacy risk assessment".

[1277] See also recital (78) ("*In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default*")

[1278] The legal binding of processors is related to the principle of accountability in the sense that it reinforces the notion of controller accountability for all personal data under its control, regardless of whether it is processed by the controller itself or by an agent on its behalf. See also OECD, *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 2013, p. 23.

[1279] See in particular also article 30(4), which provides that the controller or the processor shall make the record available to the supervisory authority on request.

which are directly relevant to processors under Directive 95/46 and the GDPR respectively:

Relevant provisions	Directive 95/45	GDPR
Applicable law	X	✓
Principles of data quality	X	X
Legitimacy of processing	X	X
Sensitive data	X	X
Transparency	X	X
Data subject rights	X	Applicable through contract (exceptions)
Co-operation with supervisory authority	Implied	✓
Data protection by design and by default	X	X
Documentation	Not specified	✓
Confidentiality	✓	✓
Security	Applicable through contract	✓
Data breach notification[1280]	X	✓
DPIA, prior authorization	X	Applicable through contract (exceptions)
Data protection officers	X	✓
Codes of conduct, certification	Not specified	✓
International transfers	Not Specified	✓
Liability	X	✓
Administrative fines	Not Specified	✓

Table 1 Comparison processor provisions Directive 95/46 – GDPR[1281]

[1280] As regards the obligation to notify data breaches, a distinction must be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller.

[1281] Legend: a check mark (✓) indicates that the provision in question is directly and expressly applicable to the actor in question; an "X" indicates that it is clear that the provision in question does not directly apply to the actor in question. The color red signals that the final text of the GDPR introduced a change in relation to Directive 95/46. The color green signal that the final text of the GDPR differs from the original EC proposal with respect to the scope of applicability of this provision.

610. RELATIONSHIP WITH CONTROLLER – Despite the increased obligations imposed upon processors, the nature of the relationship between controllers and processors has remained largely the same. As before, the processor is essentially conceived of as an "agent" or "delegate" of the controller, who may only process personal data in accordance with the instructions of the controller (articles 29 and 28(10)). Considerable detail has been added, however, as regards the legal binding of processors towards controllers (article 28(3)).

C. Relationship between joint controllers

611. APPROPRIATE ARRANGEMENT – The GDPR introduced a new provision dedicated specifically to situations of joint control. Article 26(1) provides that joint controllers must determine their respective responsibilities for compliance with the GDPR, in particular as regards the exercise of data subject rights and their respective duties to provide information, by means of an "arrangement" between them.[1282] The arrangement must duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects (article 26(2)).

612. CODIFICATION OF WP29 GUIDANCE – For the most part, article 26 of the GDPR can be seen as a codification of guidance provided by the Article 29 Working Party in Opinion 1/2010 as regards the legal implications of joint control.[1283] A notable difference, however, is that joint controllers shall in principle be jointly and severally liable towards data subjects, even if there exists an appropriate arrangement between them (article 82).

D. Cumulative liability

613. OUTLINE – Article 82 of the GDPR retained the basic principle that a controller may be held liable for damages suffered as a result of an unlawful processing activity. Contrary to Directive 95/46, however, the GDPR also recognizes processor liability. In situations involving more than one controller or processor, every controller or processor involved in the processing may in principle be held liable for the entire damage insofar as the damage results from the failure to comply with an obligation for which it is responsible. Finally, the GDPR also explicitly recognizes the eligibility of non-material damages.

614. CONTROLLER LIABILITY – The liability model for controllers essentially remained the same as under Directive 95/46. A controller shall in principle be liable for

[1282] Joint controllers are not obliged to put in place such an arrangement in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.
[1283] Compare *supra*; nr. 149.

any damages arising from the unlawful processing personal data. The liability of the controller is still "*strict*" in the sense that, once an infringement has been established, the controller cannot escape liability simply by demonstrating the absence of personal fault.[1284] In addition, the controller can still be held liable for unlawful processing activities undertaken by the processor (article 81(2)). An important clarification, however, is provided by recital (146). Recital (146) specifies that in cases where a controller and processor has been joined to the same judicial proceedings, compensation may be *apportioned* according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. In cases where the processor is not joined in the same proceeding, the controller is entitled to claim back from the processor any compensation that was paid for damages for which the processor was responsible (article 82(5)).

615. PROCESSOR LIABILITY – The liability exposure of processors is more limited in scope than the liability exposure of controllers. Whereas controllers can in principle be held liable for damages arising from *any* infringement of the GDPR, processors can in principle only be held liable in case of failure to comply with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller (article 82(2)). This is essentially a *proportional liability* model, as the processor can only be held liable in relation "for its segment" in the processing.[1285]

616. CUMULATIVE LIABILITY – Article 82(4) provides that every controller or processor involved in the processing may be held liable "*for the entire damage*"[1286]

[1284] As indicated earlier, the characterization of the controller's liability as being a form "strict" liability is somewhat misleading, given that the data subject must still demonstrate existence of unlawful processing activity, which essentially amounts to a demonstration of "fault" for tort law purposes. Cf. *supra*; nr. 129. See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report", *l.c.*, p. 58 (arguing that "*at the end of the day, the [...] GDPR create[s] little more than a basic fault-based regime for privacy and data protection breaches, with a reversed burden of proof*").

[1285] See Council of the European Union, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 2012/0011 (COD), 7586/1/15 REV 1, 10 April 2015, in particular at p. 11 (Germany); 23-24 (France); p. 27 (Croatia) and 63 (Portugal). See also Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 9083/15, 27 May 2015, p. 2 (""*As most of the obligations in the Regulation, in particular in Chapter IV, rest with controllers, in many cases the controllers will be primarily liable for damages suffered as a consequence of data protection violations. However, a data subject which has suffered damages due to unlawful processing should also have the possibility to sue directly the processor in case he knows or has strong reasons to believe the processor and not (only) the controller is in fact liable. Paragraph 1 clearly acknowledges that and leaves any person the choice to sue the controller, the processor or both. The controller can thus be the so-called single point of entry, but the data subject may choose another procedural avenue.*")

[1286] Due to the apparent confusion among DAPIX delegates regarding the concept of "joint and several" liability, the decision was made to drop the terms entirely. Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p. 3 ("*Given the fact that the concept of joint and several liability seems to mean different things to different delegations, the new drafting avoids this term altogether*.")

insofar as they can be held responsible in accordance with paragraphs 2 and 3. As a result, mere involvement in the processing is not sufficient to give rise to liability: the liability of every controller or processor is conditional upon a prior finding of responsibility in causing the damage. Only in cases where the controller or processor can be deemed responsible in accordance with paragraphs 2 and 3 of article 82 GDPR can either of them be held liable for the entire damage.[1287]

617. JOINT VS. SEPARATE CONTROL - According to article 82(2), any controller involved in the processing can in principle be held liable for the damages suffered. Read in isolation, one might assume that both joint and separate controllers can be held equally liable for the entire damage. This is not the case. While joint controllers can in principle always be held liable for damages caused by processing activities under their joint control, separate controllers can only be held liable if the damage was caused by a processing activity which was under the control of that particular controller (article 82(4)). As a result, separate controllers shall still only be liable for the entire damage in case of "concurring faults".[1288]

618. EXEMPTIONS – Article 82(3) GDPR provides that a controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. Article 82(3) GDPR echoes the escape clause of article 23(2) of Directive 95/46. Interestingly, the GDPR does not contain a recital similar to recital (55) of Directive 95/46, which provides two examples of how the controller might prove that it is not responsible "*for the event giving rise to the damage*". Nevertheless, it is reasonable to assume that the words "*not in any way responsible for the event giving rise to the damage*" should still be interpreted in the same way. As a result, the escape clause of article 82(3) refers exclusively to "*events beyond control*", i.e. an abnormal occurrence which cannot be averted by any reasonable measures and which does not constitute the realisation of the risk for which the person is strictly liable.[1289] If anything, the addition of the words "*in any way*" (in comparison to article 23(2) of Directive 95/46), suggests a desire to tighten the scope of the escape clause even further.[1290] Finally, the incorporation of the intermediary liability exemptions contained in the e-Commerce Directive by way of article 2(4) makes clear that the exemptions now also apply in cases concerning data protection liability.[1291]

[1287] See also Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015, p 3 ("*[E]ach non-compliant controller and/or processor involved in the processing are held liable for the entire amount of the damage. However a controller or processor is exempted from this liability if it demonstrates that it is not responsible for the damage (0% responsibility). Thus only controllers or processors that are at least partially responsible for non-compliance (however minor, e.g. 5%) with the Regulation, and/or in case of a processor, with the lawful instructions from the controller, can be held liable for the full amount of the damage.*")

[1288] Compare supra; nr. 143.

[1289] Cf. *supra*; nr. 128.

[1290] See also P. Larouche, M. Peitz and N. Purtova, "Consumer privacy in network industries – A CERRE Policy Report", *l.c.*, p. 58.

[1291] Pursuant to article 1(5)b of the e-Commerce Directive, it could be argued that the liability exemptions for intermediary service providers did not apply to cases concerning liability under Directive 95/46.

619. NON-MATERIAL DAMAGES – Finally, it is worth noting that article 82(1) GDPR explicitly recognises that data subjects may seek compensation for both material and non-material damages. In doing so, the EU legislature has clarified that the right to compensation extends to "non-pecuniary damages". While this was arguably already the case under Directive 95/46[1292], the clarification is nevertheless welcome with a view of removing doubt and ensuring a harmonised approach among EU Member States.

[1292] Cf. *supra*; nr. 124.

Chapter 8 CONCLUSION: DYNAMIC DEVELOPMENT OF THE CONTROLLER AND PROCESSORS CONCEPT

1 INTRODUCTION

620. OBJECTIVE – The objective of this Chapter is to synthesize how the controller and processor and processor concepts developed over time. While tracing the origin and development of both concepts, special consideration will be given to how the concepts have been used to determine the allocation of responsibility and risk. Three questions in particular shall guide the analysis:

(a) Does the instrument formally define who is responsible for compliance?

(b) How does the instrument deal with situations of outsourcing? Is there a formal recognition of agents "acting on behalf of" the entity responsible for compliance?

(c) How are responsibility and risk allocated? Is every actor subject to its own independent obligations? Or is a contractual approach adopted?

2 DEVELOPMENT OF THE CONTROLLER CONCEPT

2.1 THE MEANING OF "CONTROL"

621. ETYMOLOGY – According to Sjöblom, the term "control" was brought into the English language in the late middle ages from the French "*contre-rôle*", which meant "duplicate register".[1293] The original meaning of "control" was thus "*to take and keep a copy of a roll of accounts and to look for errors theirein*" or "*to check or verify, and hence to regulate*".[1294] By the 17th century, "control" also referred to the nature of the relationship between the verifier and the verified, signifying "mastery" over something or someone.[1295]

622. CONTROL IN THE CONTEXT OF COMPUTING – During the 1940's, computers were seen (and often designated) as "control systems".[1296] For example, computers were deployed for purposes of "gunfire control" or "inventory control".[1297] During the late 1950's, the term "control" became increasingly associated with "management control" in

[1293] G. Sjöblom, "Control in the History of Computing: Making an Ambiguous concept Useful", *IEEE Annals of the History of Computing* 2011, p. 88.
[1294] *Id.*, with reference to the Oxford English Dictionary (www.oed.com).
[1295] *Ibid*, p. 86.
[1296] *Ibid*, p. 88.
[1297] *Id.*

the context of organisational theory.[1298] In this context, the concept of "control" has been associated with the generic management process.[1299] The generic management processes comprises different elements, such as

> "*(1) setting objectives;*
>
> *(2) deciding on preferred strategies for achieving those objectives, and then*
>
> *(3) implementing those strategies while*
>
> *(4) making sure that nothing, or as little as possible, goes wrong*".[1300]

Both meanings of "control" also found their application in the context of computing and, eventually, in the context of data protection law. As Sjöblom observes:

> "*[C]ontrol suggests agency – that someone is using computer-based systems to control something and achieve a certain objective […] With its undertone of domination, control helps highlight issues of power relations inherent in computer use […].*"[1301]

In the data protection context, the "controller" is viewed as an entity which processes personal data to achieve a certain objective, deriving outputs from inputs to further its organisational mission. A controller is also the entity "in charge" of the processing, even when he decides to enlist a third party (the processor) to process the personal data on its behalf. Finally, exercising control over the processing of personal data can also serve to exercise control over the individuals concerned (e.g., in the form surveillance, or the granting or withholding of privileges).

2.2 NATIONAL LAWS BEFORE 1981

623. NO FIXED TERMINOLOGY – Before the term "controller" became a legal term of art, those responsible for ensuring compliance with data protection laws went by many names. By 1980, more than a third of the then 24 OECD member countries had adopted national data protection legislation.[1302] None of these laws employed a term which etymologically resembled the word "controller". Instead, the laws either did not formally define the actors responsible for compliance (e.g., Hesse[1303], France[1304], Norway[1305],

---

[1298] *Id.*

[1299] K. A. Merchant and D.T. Otley, "A Review of the Literature on Control and Accountability", in C. S. Chapman, A. G. Hopwood and M. D. Shields (eds.), *Handbook of Management Accounting Research,* Vol. 2, 2007, Amsterdam, Elsevier, p. 785, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.2733&rep=rep1&type=pdf (last accessed 26 April 2016).

[1300] *Id.*

[1301] G. Sjöblom, "Control in the History of Computing: Making an Ambiguous concept Useful", *l.c.*, p. 88.

[1302] Organisation for economic co-operation and development (OECD), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 8. The countries were: Sweden (1973), the United States (1974), Canada (1976), Germany (1977), Denmark (1978), Norway (1978), France (1978), Austria (1978) and Luxembourg (1979).

[1303] Cf. *supra*; nr. 235.

[1304] Cf. *supra*; nr. 324.

Denmark[1306]), or used varying terminology for doing so (e.g., "responsible keeper"[1307], "storing authority"[1308], "client"[1309], or "owner"[1310]).

624. RECURRING ELEMENTS – Despite the notable differences in terminology, there were two recurring elements in the language used by national legislatures which determined how responsibility should be allocated. The first element is the element of *mastery*: the entity designated for compliance had the ability to exercise power over the processing, in one form or another. Specifically, the entity may be "*entitled to exercise control*" (Hesse), enjoy a "*power of disposal*" (Sweden) or have "*the ability to decide about the creation*" of the processing (France). A second recurring element involves the concept of *gain*: responsibility was bestowed upon the entity which reaps the benefits of the output of the processing. For example, the processing is being carried out *for "the purposes" or "activities" of the entity concerned* (Sweden), or the data are being processed "*for his account*" (Germany, France).

625. TECHNOLOGICAL MINDSET – Data protection laws adopted prior to 1981 are characterized by their use technical jargon.[1311] The laws often referred to rather technical concepts such "registers" (Sweden), "files" (France) and "databanks" (Luxembourg). A possible explanation for the differences concerns the prevailing perceptions regarding the state of the art in computing at the time the legislation was adopted. Commentators frequently highlight that the mental models and concepts underlying the terminology used by the legislature are in some way a by-product of its historical context.[1312] According to Mayer-Schönberger, for example, the first generation of data protection laws were tailored regulate the central data processing centres and

---

[1305] See § 23 of Act no. 48 of 9 June 1978 relating to personal data filing systems, English translation available at http://app.uio.no/ub/ujur/oversatte-lover/data/lov-19780609-048-eng.pdf (last accessed 2 May 2016).

[1306] See § 20 of the Private Register Act ("*lov om private register*") of 8 June 1978 (nr. 293), accessible at http://www.datatilsynet.dk/internationalt/groenland/lov-om-private-registre-mv (last accessed 2 May 2016).

[1307] See section 8 et seq. of the Swedish Data Act (Datalagen) SFS 1973: 289. See also *supra*; nrs. 275 et seq.

[1308] See paragraph 2(3) of the Federal Data Protection Act of 27 January 1977, *BGBl.* I Nr. 7 S. 201, which defined the "speicherende Stelle" as "*anyone who stores data on its own account [for its purposes] or has data stored by others*".

[1309] See article 2, §3 of the Federal Act of 18 October 1978 on the protection of personal data, *Bundesgesetzblatt für die Republik Österreich* 1978, 193. Stück, p. 3619.

[1310] See article 2 of the Law of 31 March 1979 regulating the use of personal data in automated data processing, *Journal Officiel du Grand-Duché de Luxembourg* 11 April 1979, N° 29, p. 581.

[1311] V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 224.

[1312] See e.g. Home Office (Great Brittain), *Report of the Committee on Data Protection*, *o.c.*, p. 14; J. Bing, "A Comparative Outline of Privacy Legislation", *l.c.*, p. 157; N. Lenoir, "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des libertés: Éléments pour un premier bilan de cinq années d'activité", l.c., p. 464; D.H. Flaherty, Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, & the United States, p. 175; Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, *o.c.*, p. 14-29; J. Bing, "Data Protection in a Time of Changes", in W.F. Korthals Altes a.o. (eds.), *Information law towards the 21st Century*, Information law series 2, Kluwer Law and Taxation Publishers, Deventer, 1992, p. 247 et seq; and V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 223.

centralized data banks envisioned at the time.[1313] The same vision permeated the often technical terms and concepts used in these laws, such as "data bank", "data file" or "data record".[1314] Bing similarly points out that early data protection laws reflected a "dated view" of technology, which concerned itself primarily with visions of large mainframes with files maintained by punch cards.[1315]

2.3 *INTERNATIONAL INSTRUMENTS*

626. FIRST APPEARANCE – The term "controller" became a term of art in data protection policy circles in the course of the discussions surrounding the preparation of Convention 108 and the OECD Guidelines.[1316] Speaking at an OECD symposium in 1977, F.W. Hondius, a representative of the Directorate of Legal Affairs of the Council of Europe, commented on the difficulties in developing a common understanding of key concepts as follows:

> "*The main difficulty we encountered in preparing this draft was, to use a computer term, to create interfaces between widely different concepts of the various national legal systems. […] But we found it worth the effort, after having made an analytical survey of the key concepts of national legislation, to try our hand at international standards. Mr. Benjamin will be pleased to recognize, for example, his "beneficial user" concept, which is disguised in our text as "controller of the record", a clumsy English rendering of the marvellous French expression 'maître du fichier'.*"[1317]

Inspiration for the term was seemingly sourced from computer science literature, in particular the writings of Rein Turn. In his 1975 book, Hondius noted that computer scientist Rein Turn used the term "controller" to refer to what Hondius would refer to as the "user" of a data bank.[1318] Turn had also used the term "controller" in his contribution to the 1974 OECD seminar on Policy issues in data protection and privacy[1319], as well as in anterior publications (dating back at least to 1967).[1320] Turn's use of the term

---

[1313] V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 223-224.
[1314] *Id.*
[1315] J. Bing, "Data Protection in a Time of Changes", *l.c.*, p. 247 et seq. The impact of terminology should not, however, be overstated. Even when the terminology is updated (e.g. from "controller of the file" to controller of the processing"), the actual impact remains limited if the substantive provisions are not also updated to accommodate new realities.
[1316] The Committee of Experts tasked with preparing Convention 108 also comprised participants from countries outside of Europe, as well as members of the OECD Expert Group on Transborder Data Barriers and Privacy Protection. The suggestion to use the term "controller" may therefore have originated from either forum.
[1317] F.W. Hondius, "The Action of the Council of Europe with regard to International Data Protection", in OECD, *Transborder Data Flows and the Protection of Privacy*, *o.c.*, p. 260 (emphasis added). See also *supra*; nr. 370.
[1318] See F.W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 101-103.
[1319] See R. Turn, "Data security: costs and constraints", in OECD, *Policy issues in data protection and privacy. Concepts and perspectives*, *o.c.*, p. 244 et seq.
[1320] See e.g. H.E. Peterson and R. Turn, "System implications of information privacy", in Proceeding AFIPS '67, (Spring) Proceedings of the April 18-20, 1967, spring joint computer conference, ACM, New York, p. 293.

"controller" displayed strong conceptual similarity with the terms "data controller" and "controller of the file". In his contribution to 1974 OECD seminar, for example, Turn defined the "controller" as "*(an agency) with authority over the data-base system, which specifies the population of subjects, type of data collected, and the protection policies*"[1321]. It stands to reason that the terms "controller of the file" and "data controller" were imported from computer science literature.[1322]

627. SUBTLE DIFFERENCES – Even though strong similarities exist between the definitions of the terms "controller of the file" (Convention 108) and "data controller" (OECD Guidelines), they are not identical. In particular, the terms used to describe the object of a controller's decision-making power are slightly different. Under the OECD Guidelines, the data controller decides about the *"contents and use*" of personal data.[1323] Under Convention 108, the controller of the file decides about the *purposes of the file*, the *categories of personal data* that will be stored, and the *nature of the operations* applied to those data. A second difference between the Convention and the Guidelines concerns the technological imagery that is used. Whereas the OECD Guidelines focussed on the "processing" of personal data, Convention 108 used even more technology-laden terms such as "automated data file", "automatic processing" and "controller of the file". The Convention's reliance on the notion of a "file" would soon be perceived as antiquated. Speaking at a 1982 conference on problems relating to the development and application of data protection law, Paul Sieghart argued that the very notion of a "file" was already out of date:

> "*What is relevant isn't the file, any more than the computer installation, or indeed even the content of the file or of the installation. What is important is the activity, the task, the application for which the original data are being used, and what one gets to once again is the question of encouraging the right information flows, and seeking to discourage the wrong ones*".[1324]

Other commentators similarly observed that the idea of centralized data banks was "an idea which belongs to yesterday"[1325] One should no longer think in "monolithic" and "unitary" terms when it comes to data protection[1326], but instead think in terms of processing operations and information processing systems.[1327]

[1321] R. Turn, "Data security: costs and constraints", *l.c.*, p. 244.
[1322] See also *supra*; nr. 370.
[1323] Cf. *supra*; nr. 367.
[1324] Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, *o.c.*, p. 16-17.
[1325] *Ibid*, p. 20.
[1326] Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, *o.c.*, p. 14-15
[1327] *Ibid*, p. 27(noting that the French data protection authority, the CNIL, was increasingly called upon to pronounce itself over the use of networked information systems, rather than over the creation of "files")

2.4 NATIONAL LAWS AFTER 1981

628. UK AND BELGIAN DATA PROTECTION ACTS – Interestingly, the UK Data Protection Act (1984) adopted neither the term "controller of the file" nor the term "data controller". Instead, it employed the term "data user", a term similar to the term "databank user" which had featured in previous Council of Europe documents.[1328] Terminological differences aside, the definition of a data user in the 1984 UK Act was substantively very similar the definitions contained in the OECD Guidelines and Convention 108.[1329] The Belgian Data Protection Act (1992) more closely mirrored both the terminology and definition of the "controller of the file" contained in Convention 108.

629. RECOGNITION OF SHARED CONTROL – The 1984 UK Data Protection Act formally recognized that the processing might be controlled by more than one entity. It did so by defining the data user as a person who "*either alone or jointly or in common with other persons*" controls the contents and use of the data. The Act thus immediately distinguished two types of shared control, namely "joint control" (whereby control is exercised by several data users acting together) and "control in common" (whereby several users share a pool of information, but each use the information for his own purposes independently of the other).[1330] The Belgian Data Protection Act of 1992 did not formally recognize the possibility that the decision-making power over the processing might be exercised by more than one entity.[1331] Commentators soon observed, however, that there may be situations in which it is impossible to appoint a single controller (particularly in cases where different sets of processing activities were wholly or partially integrated with one and other).[1332]

2.5 DIRECTIVE 95/46 AND THE GDPR

630. FROM "FILE" TO "PROCESSING" – The initial Commission proposal for a European Data Protection Directive defined its scope in terms of "data files". The continued use of the term "file" was soon criticized, however, by the members of the Economic and Social Committee, who noted felt that the concept was too narrow.[1333]

[1328] See the Explanatory Report accompanying Council of Europe Resolution (73)22 regarding private sector data banks, paragraph 15.

[1329] Although the formal definition of a data user referred to the "contents and use" (similarly to the OECD definition), the explanation of these terms mapped with the definition of Convention 108 (item and type of data to be recorded, purposes)

[1330] Cf. *supra*; nr. 433.

[1331] To the contrary, the preparatory works clearly indicate that the purpose of the definition was to arrive at a single controller for each processing.

[1332] Cf. *supra*; nr. 467.

[1333] Economic and Social Committee, "Opinion on: the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data; the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks;

The Committee felt that the concept of "processing of personal data" rather than "file" should be used to define the scope of the Directive.[1334] The Commission readily agreed on the grounds that the concept of a "file" was outdated and irrelevant given the development of automation and telecommunications.[1335] The amended Commission proposal thus passed from a "static" definition linked to concept of a file to a more "dynamic" definition linked to the processing activity.[1336]

631. FROM "DATA, OPERATIONS AND ACCESS" TO "MEANS" – In the Commission's original proposal, the role of controller would stem from determining four elements: objectives, personal data, operations and third parties having access to them.[1337] The Council reduced the four elements to two, by referring only to the "purposes and means".[1338] According to the Article 29 Working Party, the practical significance of this change should not be overstated:

> *The final formulation of the provision, referring only to "purposes and means", cannot be construed as being in contradiction to the older version, as there cannot be any doubt about the fact that e.g. the controller must determine which data shall be processed for the envisaged purpose(s). Therefore, the final definition must rather be understood as being only a shortened version comprising nevertheless the sense of the older version. In other words, "means" does not only refer to the technical ways of processing personal data, but also to the "how" of processing, which includes questions like "which data shall be processed", "which third parties shall have access to this data", "when data shall data be deleted", etc.*[1339]

632. RELATIONSHIP "PURPOSE" AND "MEANS" – The definition of a controller in Directive 95/46 treats the elements of "purpose" and "means" as equal. Strictly speaking, it does not attach greater weight to either element. Nevertheless, scholars and regulators soon began to emphasize the importance of the element of "purpose" over the element of "means".[1340] This tendency can be explained in part by a desire to be pragmatic (to accommodate the fact that entities that process personal data "on behalf"

---

and — the proposal for a Council Decision in the field of information security (91/C 159/14)", *O.J.* 17 June 1991 C 159/40.

[1334] *Id.*

[1335] See Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, p. 3. See also D. Bainbridge, *EC Data Protection Directive*, *o.c.*, p. 25.

[1336] Opinion 1/2010, *l.c.*, p. 13

[1337] *Ibid*, p. 14

[1338] *Ibid*, p. 13

[1339] *Ibid*, p. 14.

[1340] See D. De Bot, *Verwerking van persoonsgegevens*, *o.c.*, p. 46 and Office of the Information Commissioner, "Data Protection Act, 1998 - Legal Guidance", Version 1, not dated, 16, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf) (last accessed 26 November 2010). Bainbridge has even raised the question as to whether it might have been better to identify the controller based on who determines the purposes alone (See D. Bainbridge, EC Data Protection Directive, *o.c.*, p. 128.). Proposals in this sense were also made during the legislative process surrounding the GDPR. Cf. *supra*; nr. 553.

of other entities often substantially influence the means of the processing). A more compelling justification for this approach is the fact that the finality pursued by (a set of) processing operations fulfils a fundamental role in determining the scope of the controller's obligations, as well as when assessing the overall legitimacy and/or proportionality of the processing (see in particular article 6, 1 (b) through (e) and article 7 (b) through (f) of the Directive).[1341] In the end, it is the "purpose" of the processing which establishes whether the collection of personal data is legitimate.[1342]

633. STRATEGIC IMPORTANCE OF "MEANS" – Despite several proposals to remove the reference to "means" from the definition of controller[1343] in the GDPR, it was decided to keep both elements. The EDPS argued that both elements should be retained, as they have both "contributed to the understanding and delineation of the roles of controllers and processors".[1344] In my view, there is also a strategic dimension related to the element of "means". Deleting "means" would arguably make it more difficult to qualify third party service providers as "controllers". Specifically, the deletion of "means" would make it easier for service providers who effectively determine the "means" of the processing (but have limited interest in the purposes pursued by their clients) to argue that their influence over the processing does not warrant a qualification as (co-)controller.[1345] The Working Party's distinction between "essential" and "non-essential" can more readily be understood when viewed in this light.

634. MULTIPLICITY OF CONTROL – An important characteristic of Directive 95/46 was its recognition of shared or "joint" control. The EU legislature mainly envisioned situations whereby a number of parties jointly determine the purposes and means of the processing as a whole. According to the Article 29 Working Party, however, full joint

---

[1341] For a comprehensive analysis of the fundamental role that the finality principle plays within data protection regulation see S. Gutwirth, "De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", *l.c.*, p. 1409-1477 and S. Gutwirth, *Privacy and the information age*, *o.c.*, p. 97-102.

[1342] Economic and Social Committee, "Opinion on: the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data; the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks; and — the proposal for a Council Decision in the field of information security (91/C 159/14)", *l.c.*, p. 40.

[1343] See European Parliament, Opinion of the Committee on Industry, Research and Energy (ITRE), 26 February 2013, Amendment 80; Opinion of the Committee on Internal Market and Consumer Affairs (IMCO), 28 January 2013, Amendment 62; Opinion of the Committee on Legal Affairs (JURI), 25 March 2013, Amendment 38 and European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendments 746-48 . The deletion of "means" had was also supported by the authors of an External Report commissioned by the European Parliament: see X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31 and the arguments provided there.

[1344] European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", 15 March 2013, p. 6 (at paragraph 24), accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf (last accessed 20 October 2015).

[1345] See also MEP amendment 748, which justified the deletion of means as follows: "*The aim of the change is not to lower the level of protection for the individual but to clarify that only the controller and not the processor is responsible. See related Amendments to articles 22, 24, 26 and 77.*"

control, whereby by all controllers equally determine the purposes and means of the processing, is only one of many different kinds "pluralistic" control. [1346] Faced with the increasing complexities of data processing, the Working Party took upon itself the task of differentiating between the different forms in which shared control might manifest itself. Arguably, the Working Party has at times gone farther in its interpretation of the controller concept than initially contemplated by the drafters of Directive 95/46.[1347]

635. APPROACH OF THE GDPR – The increasing complexity of modern processing operations led several commentators to question the continued viability of both the controller and processor concepts. In the end, however, the EU legislature followed the viewpoint of the Article 29 Working Party who considered that the concepts themselves remained valid.[1348] Legislative changes instead focused on the obligations and implications associated with each concept, resulting in more specific provisions as regards the obligations, responsibilities and liability of both controllers and processors.[1349] The legislative changes also codified parts of the guidance provided by the Article 29 Working Party under Directive 95/46 (e.g., rules on joint control) and confirmed certain general principles of tort law (e.g., rules on "cumulative" liability). The following section, which analyses the development of processor concept, will further clarify how the distribution of responsibility between controllers and processors evolved over time.

3 DEVELOPMENT OF THE PROCESSOR CONCEPT

3.1 NATIONAL LAWS BEFORE 1981

636. DELEGATION AND OUTSOURCING – From the very first data protection laws, policymakers were mindful of the fact that data processing frequently involved outsourcing. Although the Hessian Act of 1970 did not formally define the concept of a "processor", it did refer to the "*operators of data processing centres*" and persons responsible for implementing the processing ("*betrauten personen*"). The Swedish Data Act also made mention of persons and organisations who handled personal registers "on behalf of" a responsible keeper. Nevertheless, the "processor", understood as a third party who processes data as a service to others, was mainly present in the background.

[1346] Opinion 1/2010, *l.c.*, p. 18.
[1347] See also L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, Oxford, Oxford University Press, 2012, p. 220-222.
[1348] Opinion 1/2010, *l.c.*, p. 33 ("*In its analysis, it has emphasized the need to allocate responsibility in such a way that compliance with data protection rules will be sufficiently ensured in practice. However, it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable in that perspective.*") and European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2, *l.c.*, p. 10.
[1349] European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2, *l.c.*, p. 10.

It was not until the late 1970's that so-called "computer service bureaux" or "computer service agencies" gained more formal recognition in national data protection laws.[1350]

637. EXECUTION VS. AUTHORITY – The "power to decide" and the "ability to act" do not necessarily coincide. The early data protection laws differentiated between those entitled to make strategic decisions about the processing of personal data and those who merely execute instructions. For example, section 3 of the Hesse Data Protection Act implied that the decision-making power over the disclosure of data may lie elsewhere than with the actual holders of the data. In the Swedish Data Act, the definition of a "responsible keeper" was designed to target the entity that actually "controlled" the register, as opposed to those who were merely passively following instructions.[1351] The French LIFL repeatedly differentiated between, on the one hand, the entity that "*decided about the creation of data processing*", "*ordered*" or "*had others carry out*" personal data processing, and, on the other hand, the entities who might be engaged in the processing of personal data on behalf of others (i.e. the entities "*performing the processing*", the "*holders*" of the files).

638. ACCOUNTABILITY OF THE PRINCIPAL – The early data protection laws implicitly embraced the notion that when someone engages a third party to process personal data on his behalf, he remains responsible for ensuring compliance. For example, the Hesse Data Protection Act, which in principle applied only to the public sector, also found application in situations where a public authority commissioned a private entrepreneur to process data on its behalf.[1352] In the same vein, the Swedish Act Data Act provided for strict liability of the "responsible keeper" in cases where an individual suffered harm because of inaccurate data, regardless of whether the processing of data had been outsourced or not.[1353]

639. SUBJECT TO REGULATION – While the entity possessing the power to decide about the processing may have been "ultimately" responsible for compliance, those involved in the implementation were by no means exempted. The privacy laws of Hesse, Sweden and France all allocated certain responsibilities upon entities acting "on behalf

---

[1350] The "computer service agency" was formally recognized by §20 of the Danish Act no. 293 concerning private registers of 8 June 1978 ("Lov om private registre m.v."); whereas § 22 of Norwegian Act no. 48 of 9 June 1978 relating to personal data filing systems formally regulated "data processing enterprises".

[1351] In the early stages of the preparation of the Swedish Act, the term "file keeper" had been used in lieu of the term "responsible keeper". The replacement was reportedly made because the term "responsible keeper" made it clearer that the term referred to the party that actually controlled the file and made decisions on its contents. The concept therefore excluded service bureaus and other parties that might have been involved in the processing of a personal register without actually "controlling" it. (see P.G. Vinge, *Swedish Data Act*, *o.c.*, p. 9.)

[1352] Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, *l.c.*, p. 11. The Data Protection Commissioner emphasized that in case of outsourcing the public authorities concerned remained responsible and accountable for the implementation of appropriate data protection measures. (*Ibid*, at p. 33.) ("*Verantwortlichkeit der Verwaltungen - Entgegen manchen Äusserungen und Erwartungen ist daran zu erinnern, dass die volle verantwortung für die Durchführen des Datenschutzes den Behörden und Stellen obliegt, die mit der maschinellen Datenverarbeitung befasst sind.*")

[1353] Cf. *supra*; nr. 268 and 284.

of" the responsible entity, whether they were acting in the capacity of a service provider or as an employee.[1354] For the most part, their responsibilities were limited to (a) duties of confidentiality; (b) an obligation to ensure security of processing; as well as (c) a general duty to co-operate with supervisory authorities.[1355]

3.2 INTERNATIONAL INSTRUMENTS

640. PROCESSORS NOT REGULATED – Neither Convention 108 nor the OECD Guidelines formally defined the concept of a "processor", nor did they assign any responsibility to the entities acting "on behalf" of the controller. The Explanatory Memoranda made clear that "service bureaux" or persons who merely carry out the instructions issued by a controller were not targeted by either instrument. In case of the OECD Guidelines, however, the Explanatory Memorandum explicitly noted that Member countries remained free to develop "more complex schemes of levels and types of responsibilities" when implementing the Guidelines[1356]:

> "*[…] nothing in the Guidelines prevents service bureaux personnel, "dependent users" […] and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information […].*"[1357]

641. CONTROLLER ACCOUNTABIILTY – The controller retained his responsibilities, under both Convention 108 and the OECD Guidelines, when engaging a third party to process personal data on his behalf. This premise was most explicit in the definition of a "data controller" in the OECD Guidelines, which defined the data controller as the party who is competent to decide about the contents and use of the data, "*regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf*." The principle of accountability (paragraph 14) further

---

[1354] Cf. *supra*; nr. 239 (Hesse); nr. 283 (Sweden) and nr. 329 (France).

[1355] Still, notable difference existed between the three acts. Under the Hessian Act, responsibility for ensuring compliance with the Hesse Data Protection Act was shared, at least in part, by all entities involved in the preparation and execution of automatic data processing. While the Swedish Data Act imposed fewer obligations upon those who merely executed the processing, two of its provisions explicitly targeted persons or organisations acting "on behalf of" a responsible keeper (duty of confidentiality, duty to co-operation with the Data Inspection Board). The French LIFL imposed a wider range of obligations upon persons or organisations processing personal data on behalf of others, ranging from an obligation to maintain the security of processing, to the duty to co-operate supervisory authorities and the accommodation of data subject rights.

[1356] Organisation for economic co-operation and development (OECD), Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, paragraph 40.

[1357] Organisation for economic co-operation and development (OECD), Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, paragraph 62. For a detailed discussion of the "processing services" and "data services" offered by "computer service bureaux" at the time see J. Bing, P. Forsberg and E. Nygaard, "Legal problems related to transborder data flows", in OECD, *An Exploration of Legal Issues in Information and Communication Technologies*, *Information Computer Communication Policy* nr. 8, Paris, OECD, 1983, p. 129-131.

reinforced the notion that the data controller remained responsible even when the processing was to be outsourced to a third party.

3.3 NATIONAL LAWS AFTER 1981

642. FORMAL RECOGNITION – Data protection laws after 1981 (e.g. UK, Belgium, and Netherlands) formally recognized "processors" as separate entities, worthy of their own statutory definition. National laws varied significantly, however, as to the extent to which they imposed obligations directly upon these entities.

643. UK DATA PROTECTION ACT – From its inception, the drafters of the UK Data Protection Act foresaw responsibilities for both "data users" and "computer bureaux". Despite lobbying efforts by the computer services industry, the House of Lords wound up rejecting the notion that computer bureaux should be left outside the scope of the Act. Computer bureaux would be subject to the Act, but would have far fewer responsibilities bestowed upon them. Computer bureaux were mainly obliged to (1) register their activities; (2) act in conformity with instructions of the data user as well as the terms of the relevant register entries; and (3) ensure the security of processing. The remainder of the obligations provided under the Act were directed almost exclusively to data users. Nevertheless, bureaux were subject to the supervision of the Registrar and were exposed to the risk of both civil and criminal liability for activities residing within their sphere of control. A similar approach was adopted in the Netherlands under the Dutch Data Protection Act of 1988.[1358]

644. BELGIAN DATA PROTECTION ACT – The Belgian Data Protection Act of 1992 recognized the concept of a "processor", but did very little with it in terms of further regulation. The main purpose of the term was seemingly to reinforce the responsibility of the controller, regardless of how the processing was organized.

645. AGENCY – The definition of a "computer bureau" in the UK Act made clear that the any processing of personal data by the bureau occurred on an agency basis. According to the Data Protection Registrar, however, "agency" in this context merely meant "*a person acting for others*" rather than as an agent in a contractual sense.[1359] Because a computer bureau acted "on behalf" of a data user, it was in principle not allowed to disclose personal data without prior authorization by the data user who controls that data.[1360]

[1358] For more information see A.C.M. Nugter, *Transborder Flow of Personal data within the EC*, *o.c.*, p. 171-172.

[1359] The Data Protection Registrar, "The Data Protection Act 1984: The Definitions", *l.c.*, p. 12.

[1360] See also HL Deb, 21 July 1983, vol. 443, at cc 1299-1300, accessible at http://hansard.millbanksystems.com/lords/1983/jul/21/data-protection-bill-hl#S5LV0443P0_19830721_HOL_155 (discussing the exemption to the non-disclosure requirement for access requests by law enforcement and its relationship to computer bureaux).

3.4 DIRECTIVE 95/46 AND THE GDPR

A. Directive 95/46

646. ROLE OF THE PROCESSOR – Although not defined in the initial Commission proposal, the final version of Directive 95/46 defined the "processor" as a separate entity. The motivation for regulating "processing on behalf of the controller" was to avoid situations whereby processing by a third party on behalf of the controller would have effect of reducing the level of protection enjoyed by the data subject.[1361] According to the Article 29 Working Party, the processor concept wound up serving a dual purpose within the framework of Directive 95/46, namely:

a) to identify the responsibilities of those entities who are closely involved in the processing, but are doing so on behalf of one or more other entities (controller(s));

b) to help distinguish between those entities that are responsible for compliance on the one hand, and those entities that are merely executing the instructions they have been given.[1362]

647. AGENCY – The main substantive component of the processor concept is that a processor acts "on behalf" of a controller. The Article 29 Working Party has approximated this wording with the legal concept of delegation, whereby one entity requests another entity to undertake certain actions on its behalf.[1363] Directive 95/46 implicitly views processors as passive agents, who merely execute instructions received from the controller and have no determinative influence over the processing. This explains why the Directive imposes only the limited obligation of adhering to instructions issued by the controller.

648. LIMITED ACCOUNTABILITY – Under Directive 95/46, responsibility for compliance rests entirely with the controller. Processors are in principle only indirectly responsible, by virtue of a contract or other legal act which binds them to the controller. Earlier draft versions of the Directive foresaw a number of obligations that would be directly incumbent upon processors. In the final version, however, only one obligation remained, namely the duty not to process personal data except on instructions from the controller (article 16). Directive 95/46 also did not afford data subjects with direct recourse against processors (although such recourse could be provided by national law).

649. CONTRACTUAL SAFEGUARDS – The extent to which the processor complies with the substantive norms of Directive 95/46 hinges primarily upon the contractual safeguards which are put in place. Article 17(3) of the Directive obliges controllers to

[1361] Cf. *supra*; nr. 489.
[1362] Opinion 1/2010, *l.c.*, p. 7.
[1363] *Id.*

put in place a contract or other legal act "binding the processor to the controller", which must specify that the processor is obliged (1) to follow the controller's instructions at all times and (2) to implement appropriate technical and organisational measures to ensure the security of processing. Article 17(3) only mentions the minimum content that should be included in an arrangement between controllers and processors, so it is not excluded that controllers bind their processors to additional data protection principles or safeguards.

B. GDPR

650. CONCEPTS INTACT – The proposal of the European Commission left the concepts of controller and processor intact.[1364] As indicated earlier, the Commission considered the concepts themselves to be largely unproblematic.[1365] The proposed changes instead focused on (a) specifying the obligations of each actor in greater detail; (b) defining additional obligations for processors; and (c) addressing the relationship between joint controllers.[1366]

651. DIRECT AND INDIRECT ACCOUNTABILITY – The GDPR retains the general principle that the controller carries "primary" or "overarching" responsibility for ensuring compliance. It also recognizes, however, that processors can play an important role in ensuring compliance. The GDPR imposes a number of obligations directly upon processors, without necessarily making them dependent on the existence of a "contract or other legal act" between the controller and processor. While contractual safeguards continue to play an important role, the enforceability of certain obligations is no longer contingent upon the existence of such arrangements. For example, with or without a contract, processors are obliged to maintain documentation, ensure an appropriate level of security and co-operate with supervisory authorities. Processors are also directly liable towards data subjects with respect to the activities that fall under their responsibility.

652. MORE CONTRACTUAL SAFEGUARDS – The GDPR provides that the relationship between controllers and processors must be governed by a contract or legal act which binds the processor to certain obligation vis-à-vis the controller. In comparison to Directive 95/46, the number of elements to be included in the arrangement between controllers and processors has increased considerably. Under article 28(3), the arrangement must at a minimum specify the subject-matter and duration of the

[1364] The Commission only proposed one minor change to definition of a controller, namely adding the word "conditions". See also P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review* 2012, vol. 28, p. 133 and P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143.

[1365] Cf. *supra*; nr. 531.

[1366] See also P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 133.

processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. Other mandatory elements include, but are not limited to: the obligation to process personal data only on instructions of the controller (including in relation to international transfers); the obligation to respect restrictions regarding sub-processing; and the obligation to delete or return all the personal data to the controller after the end of the provision of services.

653. AGENCY – The GDPR did not deviate from the fundamental premise that the processor should be viewed as an "agent" of the controller and therefore must be bound to adhere to the controller's instructions unless required by law to act otherwise. As a result, the controller in principle remains liable for the actions performed by the processor. The processor faces independent liability, however, in case of failure to comply with its legal obligations or controller instructions (article 82(2)).

PART IV

USE CASES

Chapter 1 INTRODUCTION

"*A functional theory does not necessarily translate into a successful practice*".

- *Jonathan Zittrain*[1367]

654. PREFACE – For more than 20 years, the controller-processor model of Directive 95/46 has provided the analytical template for the allocation of responsibility and risk among actors involved in the processing of personal data. While the model itself appears conceptually sound, its application in practice has not always been straightforward. The research objective of this Part of the thesis is to identify the main issues that surround the practical application of the controller-processor model. To this end, a number of real-life use cases will be examined.

655. SELECTION CRITERIA – Needless to say, it is impossible to document and analyse every possible use case. A selection needs to be made. In social science research, case selection is generally driven by two objectives, namely (1) *representativeness* (i.e., ensuring that the selected cases are sufficiently representative in light of the research question) and (2) *variety* (i.e., ensuring useful variation on the dimensions of theoretical interest).[1368] A third, sometimes implicit, objective is *relevancy* (i.e., ensuring that the selected use cases are likely to yield insights which can assist in answering the research question).[1369]

656. RELEVANCY – As the research objective of this Part of the thesis is to document the issues that arise when applying the controller-processor model in practice, the pool of potentially relevant use cases is limited to instances in which such issues occur. In the first phase of selection, a preliminary literature study was undertaken to identify eligible use cases. The threshold for eligibility was the existence of some indication, either in regulatory guidance or doctrine, that the use case in question challenges either the application of the controller and processor concepts or the associated allocation of responsibility and risk.[1370] Each of the retained use cases has been cited by scholars

---

[1367] J. Zittrain, "Privacy 2.0", *University of Chicago Legal Forum* 2008, No. 1, article 3, p. 68, available at http://chicagounbound.uchicago.edu/uclf/vol2008/iss1/3/ (last accessed 20 April 2016).

[1368] J. Seawright and J. Gerring, "Case Selection Techniques in Case Study Research – A Menu of Qualitative and Quantitative Options", *Political Research Quarterly* 2008, Vol. 61, No. 2, p. 296.

[1369] Seawright and Gerring refer to this as "purposeful" (as opposed to "random") selection of case studies. (*Ibid*, p. 295). For additional information regarding criteria for case selection see R.K. Yin, *Case Study Research – Design and Methods*, 2009, London, Sage Publications, Fourth Edition, p. 91-92; R.K. Yin, *Applications of Case Study Research*, 2012, London, Sage Publications, Third Edition, p. 32-39; D.R. Hensler, *Designing Empirical Legal Research: A Primer for Lawyers*, 2011, second revision, p. 101-105 and A.L. George and A. Bennet, *Case Studies and Theory Development in the Social Sciences*, 2005, London, MIT Press, p. 83-84.

[1370] It obviously can not be excluded that there may be other relevant use cases, which have not (yet) been identified by regulators or scholars as presenting issues for the practical application of the controller or processor model. This touches on the issue of representativeness, which will be discussed shortly. Before

and/or regulators as instances where the application of the controller-processor concepts can be challenging, or where the effective allocation of responsibilities and risks may be undermined.

657. VARIETY – Once the initial screening for relevancy was completed, a further selection was made with the aim of ensuring a sufficient degree of variety. In practice, the control capabilities of actors involved in the processing of personal data are shaped by the social context in which they operate (e.g., public sector, business-to-business, business-to-consumer, consumer-to-consumer). Variations in control capabilities are clearly "variables of interest" in light of the problem statement of this thesis.[1371] As a result, it was considered desirable to ensure that the selected use cases concern a variety of social contexts which involve different power dynamics and control capabilities among the actors involved in the processing of personal data.

658. REPRESENTATIVENESS – The utility of use case analysis is generally predicated, at least in part, on the proposition that the selected use cases are sufficiently representative.[1372] The analysis conducted in Part V of this thesis offers some support for the proposition that the selection of use cases made here has in fact been sufficiently representative. Part V of the thesis will analyse the proposals for change which have been put forward in the context of the review of Directive 95/46 in relation the controller-processor model. When comparing the rationale of each of these proposals to the typology of issues derived from the analysis of use cases, it appears that at least one relevant counterpart can be found in each instance.[1373]

659. SELECTED USE CASES – The four use cases which have been selected for analysis are:

(1) e-government identity management;
(2) online social networks;
(3) cloud computing; and
(4) internet search engines.

---

tackling the question of representativeness, however, it is first of all necessary to ensure relevancy and it is asserted the approach adopted here is a viable (albeit heuristic) method of doing so.

[1371] Both the "broken binary" and "threshold for control" problem statements indicate that difficulties in application of the controller-processor model occur, at least in part, due to a misalignment between, on the one hand, the roles and responsibilities of controllers and processors as defined by law and, on the other hand, their effective control capabilities in practice. Cf. *supra*; nrs. 8 et seq. The term "variables of interest" has been borrowed from D.R. Hensler, *Designing Empirical Legal Research: A Primer for Lawyers*, *o.c.*, p. 15-17.

[1372] See also J. Seawright and J. Gerring, "Case Selection Techniques in Case Study Research – A Menu of Qualitative and Quantitative Options", l.c., p. 306-307.

[1373] See also *infra*; nr. 1080.

660. ANALYSIS – Over the following chapters, each of the selected uses cases will be analysed in a structured and focused manner.[1374] First, an overview of the main types of actors and interactions will be provided. Next, the legal status and obligations of each actor shall be analysed, taking into account the different interpretations put forward by courts, regulators and scholars. Finally, at the end of each use case, an evaluation will be made of the main issues that have been identified when applying the controller-processor model to the use case in question. The identified issues will serve as the main input for the typology of issues developed in Part V.

661. SCOPE – The choice has been made to use the controller-processor model of Directive 95/46, rather than that of the GDPR, as the relevant legal framework during the analysis of use cases. There are mainly two motivations behind this approach. First, in doing so, it is possible to create a better understanding of the policy choices made by the European legislature in the context of the GDPR, which will be analysed in Part V. Second, this approach will facilitate the evaluation of whether the approach adopted by the GDPR is likely to remedy the issues which challenged the controller processor-model under Directive 95/46 or whether additional improvements may be necessary.

[1374] The analysis will be "structured" in the sense that the analysis of each use case shall be composed of the same subsections and will answer the same questions in relation to each use case. The analysis shall be "focused" in that the analysis will extend only to those aspects which are relevant for purposes of the research question which this Part seeks to address. Based on A.L. George and A. Bennet, *Case Studies and Theory Development in the Social Sciences*, *o.c.*, p. 67 et seq.

Chapter 2 E-GOVERNMENT IDENTITY MANAGEMENT

1 INTRODUCTION

662. A DEFINITION OF "E-GOVERNMENT" – Public service delivery is increasingly permeated by information and communication technologies (ICTs). ICTs are deployed for a variety of reasons: cost reduction, convenience, citizen empowerment, fraud prevention, etc.[1375] Historically, the public sector has always shown a strong interest in the use of ICT.[1376] Somewhere in the 1990s, the trend towards increased ICT usage in the public sector received the label of "e-government".[1377] E-government has been defined by the World Bank as

> *"the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government."*[1378]

663. APPLICATIONS – At a high level, one can distinguish between five types of e-government applications:

(1) *Access to information* (e.g., dissemination of information to the public through websites);

(2) *Citizen participation* (e.g., online consultations or e-petitions);

(3) *Electronic procurement* (e.g., electronic tender submissions);

(4) *Government-to-government information and service integration* (e.g., re-use of citizen data across governmental departments); and

(5) *Compliance and access to benefits* (e.g., filing of tax returns, requests for permits or social security benefits, etc.).[1379]

[1375] J. Deprest and F. Robben, *eGovernment: the approach of the Belgian federal administration*, 2003, p. 6, available at https://www.law.kuleuven.be/icri/frobben/publications/2003%20-%20E-government%20paper%20v%201.0.pdf (last accessed 28 April 2014).

[1376] As explained in Part III of this thesis, it was the increased use of ICTs by the public sector that triggered the enactment of the first data protection laws in the early 1970s. Cf. *supra*; nrs. 210 et seq.

[1377] A. Grönlund and T.A. Horan situate the origin of the term "e-Gov" in the late 1990s, alongside other "e-terms" such as e-Commerce that accompanied the Internet boom. See A. Grönlund and T.A. Horan, "Introducing e-Gov: history, definitions and issues", *Communications of the Association for Information Systems* 2004, Vol. 15, p. 713-729, available at http://www.cips.org.in/public-sector-systems-government-innovations/documents/Introducing_e_governance.pdf (last accessed 28 April 2014).

[1378] The World Bank, *Definition of E-Government*, accessible at http://web.worldbank.org (last accessed 30 April 2014).

[1379] T.A. Pardo, "Realizing the Promise of Digital Government: It's More than Building a Web Site", *Information Impact Magazine* 2000, p. 3-4, available at http://demo.ctg.albany.edu/publications/journals/realizing_the_promise/realizing_the_promise.pdf. See also Z. Fang, "E-Government in Digital Era: Concept, Practice, and Development", *International Journal of The Computer, The Internet and Management* 2002, Vol. 10, No.2, p. 4.

664. ROLE OF "IDENTITY MANAGEMENT" – The relationship between citizens and public administrations is highly personal in nature.[1380] Many governmental services – in particular those belonging to the fifth category above – require identification of their intended recipients. Most of these services also require verification of additional attributes, such as "age", "place of residence", or "professional qualification". Remote delivery of government services requires mechanisms to corroborate the identity and other attributes of the individuals concerned. This is where electronic identity management (eIDM) systems play a role. eIDM systems enable governments both to *identify* and *authenticate* the users of their systems and services.[1381]

665. NATIONAL STRATEGIES – Today, most European countries have developed – or at least launched the development of – a national identity management strategy.[1382] One of the primary objectives of these strategies is to enable remote identification and authentication of citizens. In keeping with this objective, several Member States have moved from purely paper-based identification documents towards electronic identity (eID) cards.[1383] Very often, these electronic identity cards are based on Public Key Infrastructure (PKI).[1384] For transactions which only require a low level of entity authentication assurance, alternative mechanisms such as username-password combinations and other non-PKI-based tokens are also accepted.[1385]

[1380] S.S. Garcia, A.G. Oliva, E.P. Belleboni and I.P. De La Cruz, "Current Trends in Pan-European Identity Management Systems", *IEEE Technology and Society Magazine* 2012, Vol. 31, Issue 3, p. 45.

[1381] J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), "Conceptual Framework for Identity Management in eGovernment", *FIDIS project*, Deliverable D16.1, 2008, p. 20, available at www.fidis.net (last accessed 2 May 2014).

[1382] Country profiles on national eIDM schemes within the EU have been prepared by the IDABC project and can be accessed http://ec.europa.eu/idabc/en/document/6484.html (last accessed 29 April 2014). For a more recent benchmarking study see Capgemini, IDC, Sogeti, and Politecnico di Milano, "Future-proofing eGovernment for a Digital Single Market", Final Insight Report, June 2015, Study prepared for the European Commission DG Communications Networks, Content and Technology, available at https://ec.europa.eu/digital-agenda/en/news/eu-egovernment-report-2015-shows-online-public-services-europe-are-smart-could-be-smarter (last accessed 1 December 2015). For a discussion of national identity management strategies among OECD countries see OECD, *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, 2011, p. 27 et seq., available at http://www.oecd.org/sti/ieconomy/49338380.pdf (last accessed 29 April 2014).

[1383] It is worth underlining, however, that not all European countries have adopted this approach. Most governments have built upon the existing means for identity verification offline and extended or adapted them to the online world. As a result, eID cards are mainly found in countries which have a tradition with paper-based national identity cards. Countries which do not have such a tradition have developed alternative approaches to introducing digital credentials (e.g., by building on digital credentials provided by banks). (OECD, *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, *o.c.*, p. 38-39.)

[1384] See H. Graux and J. Majava, "eID Interoperability for PEGS. Analysis and Assessment of similarities and differences – Impact on eID interoperability", *IDABC project*, 2007, p. 72 et seq., available at http://ec.europa.eu/idabc/servlets/Doc0939.pdf?id=29618 (last accessed 2 May 2014).

[1385] The Belgian government, for example, issues not only an eID card but also user-name password combinations and a "federal token". Which credential may be used for which transactions depends primarily on the level of assurance required. For a more detailed discussion see D. De Cock, B. Van Alsenoy, B. Preneel and J. Dumortier, "The Belgian eID Approach", in W. Fumy and M. Paeschke, *Handbook of eID Security. Concepts, Practical Experiences, Technologies*, 2011, Publicis, Erlangen, p. 117 et seq.

666. THE ROLE OF THE EUROPEAN UNION – Since the mid-1990s, the EU has actively sought to promote interoperability among EU public administrations.[1386] The driving force behind these initiatives has been the desire to foster greater co-operation among European public services and to enable cross-border service delivery.[1387] Inevitably, the issue of electronic identity management became increasingly important. Delivery of so-called "Pan-European e-Government Services" (PEGS), would require interoperability between national identity management systems.[1388] To achieve this objective, the EU launched a wide range of initiatives (agendas, roadmaps, action plans, research projects …) with a strong focus on eID interoperability.[1389] The guiding principle in those initiatives has been the construction of a European cross-border eIDM framework, based on interoperability and mutual recognition of national eID resources and management systems.[1390]

667. OUTLINE – The objective of this chapter is to discuss how the current data protection framework relates to e-government identity management systems. It will

---

[1386] N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *Journal of International Commercial Law and Technology* 2013, Vol. 8, No.2, p. 104. One of the first initiatives was the Interchange of Data between Administrations (IDA) programme which was launched in 1995. (Council Decision of 6 November 1995 on a Community contribution for telematic interchange of data between administrations in the Community (IDA) (95/468/EC), O.J. L 269/23, 11 November 1995, accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995D0468&from=NL, last accessed 29 April 2014. The IDA programme was eventually followed up by the IDABC and ISA programmes. See Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), *O.J.* 18 May 2004, L-181 (corrig.), p. 25-35 and Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA), *O.J.* 3 October 2009, L-260/20.

[1387] S.S. Garcia, A.G. Oliva, E.P. Belleboni and I.P. De La Cruz, "Current Trends in Pan-European Identity Management Systems", *l.c.*, p. 45.

[1388] *Id.*

[1389] N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104. The increased emphasis on eID interoperability was particularly visible in the i2010 eGovernment Action Plan and the Roadmap for a pan-European eID Framework. See European Commission, *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, SEC(2006) 511, 24 April 2006, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0173&from=EN and European Commission, A Roadmap for a pan-European eIDM Framework by 2010, 2006, v1.0, available at http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf (last accessed 2 May 2014). The Roadmap included a list of measurable objectives and milestones for the construction of such framework. It later reconfigured the objectives with the launch of the Digital Agenda, which included two important key actions in the field of eID, namely (1) a proposal for a Council and Parliament Decision on mutual recognition on e-identification and e-authentication across the EU based on online "authentication services" to be offered in all Member States; and (2) a proposal for a revision of the eSignature Directive7 with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems. (N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104-105.) This eventually led to the adoption of the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (O.J. 28 August 2014, L 257/73-114).

[1390] N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104. See also J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), "Conceptual Framework for Identity Management in eGovernment", *l.c.*, p. 61-64.

start by identifying the main actors and processes involved in e-government identity management systems. Next, it will analyse the legal status ("role") of each actor, as interpreted by policymakers, regulators and scholars. After that, two real-life examples will be presented to illustrate how data protection principles can be applied in the context of e-government identity management, as well as the practical issues that arise. The first case study concerns the Internal Market Information (IMI) System, one of the very first Pan-European e-government applications. The second case study concerns cross-border identification and authentication, in particular the measures taken so far to enable interoperability of identity management systems at pan-European level.

668. ACKNOWLEDGMENT – Certain parts of this chapter are based on book chapters which were written together with colleagues.[1391] The parts reproduced here, for the most part, correspond with my personal contributions to these book chapters. Various projects and studies have researched e-government identity management, such as the IDEM[1392] and FIDIS[1393] projects. Several of the topics discussed in this Chapter rely or build on the results of this research.

[1391] B. Van Alsenoy, E. Kindt and J. Dumortier, "Privacy and data protection aspects of e-government identity management", *l.c.*, p. 251-282 and D. De Cock, B. Van Alsenoy, B. Preneel and J. Dumortier, "The Belgian eID Approach", *l.c.*, p. 117-138.

[1392] IDEntity Management for e-government (IDEM) http://www.iminds.be/en/research/overview-projects/p/detail/idem .

[1393] Future of Identity in the Information Society (FIDIS): http://www.fidis.net.

2 ACTORS

669. SELECTION CRITERIA – The current inventory of actors is based on a literature study of the output of various research projects[1394], academic publications[1395], policy documents[1396] and international standards[1397] concerning identity management and/or e-government. A common denominator among the identified actors is that they participate in the operation of identity management systems, which can be described as

> *"the organisational and technical infrastructure used for the definition, designation and administration of identity attributes*." [1398]

670. ACTORS OVERVIEW – The following types of entities[1399] may be considered as main entities involved in the operation of e-government identity management systems:

(1) Citizen;

(2) Authoritative source;

(3) Credential Service Provider (CSP);

(4) Integrator;

(5) Verifier; and

(6) Relying Party.

[1394] E.g. the STORK (Secure idenTity acrOss boRders linKed) (https://www.eid-stork.eu); IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) (http://ec.europa.eu/idabc); FIDIS (Future of Identity in the Information Society) (http://www.fidis.net) and the LEGAL IST project.

[1395] E.g., H. Leitold and B. Zwattendorfer, ""STORK: Architecture, Implementation and Pilots", in N. Pohlmann a.o. (eds.), ISSE 2010 Securing Electronic Business Processes, Springer, 2010, p. 131-142 and D. De Cock, *Contributions to the Analysis and Design of Large-Scale Identity Management Systems*, Dissertation presented in partial fulfilment of the requirements for the degree of Doctor in Engineering, June 2011, 234 p.

[1396] E.g. J. Deprest, and F. Robben, *eGovernment: the approach of the Belgian federal administration*, *o.c.*, 57 p.

[1397] E.g. ISO/IEC Information technology -- Security techniques -- Entity authentication assurance framework, ISO/IEC 29115:2013(E), 1 April 2013, 36 p.; International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, September 2012, 44 p., available at https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11608 and International Telecommunication Union (ITU), Telecommunication Standardization Sector Focus Group on Identity Management, *Report on Identity Management Framework for Global Interoperability*, 30 p., https://www.itu.int/ITU-T/studygroups/com17/fgidm.

[1398] Modinis project, Common Terminological Framework for Interoperable Electronic Identity Management, Consultation Paper, v2.01, 23 November 2005, p. 12, accessible at https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf (last accessed 29 April 2014).

[1399] The term "entity" (instead of "actor") is used to signal that each identified "actor" could in principle be either a separate legal entity or a purely technical component operated by the same actor. For example, a Relying Party might operate its own verification service, in which case there the "Verifier" depicted in Figure 2 would not be a separate legal entity but rather a component operated by the Relying Party.

671. VISUAL REPRESENTATION – The aforementioned entities interact with each other in a variety of ways. The following figure provides a – highly simplified – representation of how these entities typically interact in the context of an e-government identity management system. It is intended to be conceptual rather than factual.

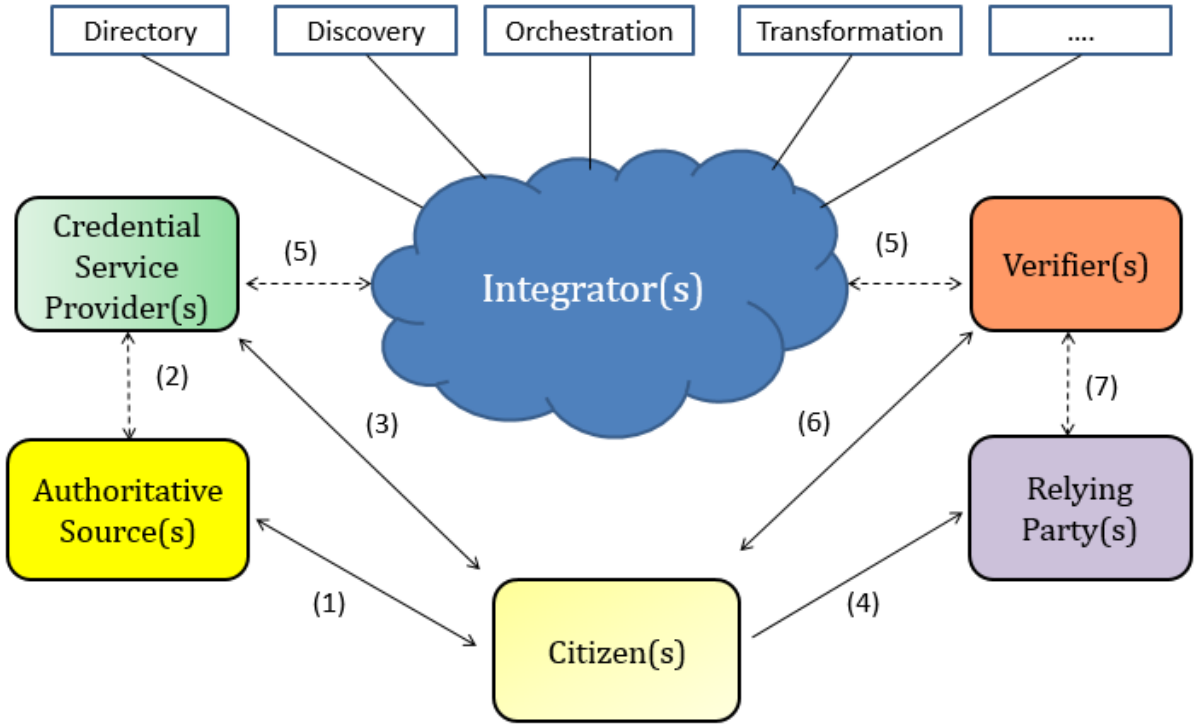

Figure 2 – Main entities in e-government identity management systems

672. LEGEND – The arrows in Figure 2 indicate that an exchange of personal data is taking place. Solid black arrows signify exchanges of personal data which occur primarily "in the foreground", meaning that they can easily be observed or inferred by citizens. They typically imply some form of active involvement by the citizen (e.g., manually entering data, use of an application). Dashed grey arrows were used to signify data exchanges which may be less obvious to citizens. Over the following sections, each of the actors and interactions displayed in Figure 2 will be briefly described.

673. COMBINATIONS POSSIBLE – The reader should note that the categories of entities identified in Figure 2 are by no means mutually exclusive. A given actor may combine multiple roles depending on the circumstances. For example, an Authoritative Source might also act as a CSP, or a Verifier might also operate its own integration service.[1400] The entities identified in Figure 2 should therefore be thought of as conceptual building blocks, which may be provided by one or more actors.

[1400] Similarly, a citizen might also operate its own "integrator", e.g. in the form of a middleware software component.

674. COMMON PURPOSE – As indicated earlier, e-government identity management systems are used to *identify* and *authenticate* individuals who make use of governmental systems or services. They may also be used to corroborate other attributes of the individuals concerned. While the actors depicted in Figure 2 may pursue any range of purposes as part of their daily activities, the following sections will focus on each entity's involvement (or "contribution") in enabling the identification and authentication of citizens' identity attributes.

2.1 CITIZEN

675. MAIN CHARACTERISTICS – In an identity management context, a citizen is understood primarily as the *subject of a digital identity*.[1401] This identity can be composed of any number of attributes (e.g., name, gender, date of birth,).[1402] As a rule, at least one of these attributes shall consist of an *identifier* which allows the citizen to be uniquely recognized within a particular context.[1403] Provided the citizen has also been issued the appropriate credentials, it will be possible to *authenticate* his or her identity remotely.[1404]

676. RELATED PROCESSES – Before creating a digital identity, a government will have collected various data about its citizens. These data are kept in one or more Authoritative Sources (see below). Standard identity data includes information such as first and last name, gender, date of birth and place of residence.[1405]

677. DATA FLOWS – The data flows which facilitate identification and authentication of citizens are represented in Figure 2 by arrows (1) through (7). Each of these data flows will be elaborated further over the following sections.

[1401] Of course, not only citizens or individuals have digital identities. An identity might also refer to a software component or device. For purposes of conceptual clarity, however, the discussion here focuses only on identities relating to citizens.

[1402] From a holistic perspective, the "identity" of an entity can be described as the dynamic collection of all attributes relating to that entity. As such, the identity of an entity is a fluid and evolving concept, rather than a practical one. Identity management systems actually focus on a specific subset of relevant attributes, commonly referred to as "partial" or "digital" identities. (Modinis project, Common Terminological Framework for Interoperable Electronic Identity Management, Consultation Paper, *l.c.*, p. 6 and 12 and the workshops held in the context of the EU FIDIS project.)

[1403] An identifier can be described as an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. (Modinis project, Common Terminological Framework for Interoperable Electronic Identity Management, Consultation Paper, *l.c.*, p. 12). An entity can be known under more than one identifier. In an e-government context, this identifier is typically assigned by a governmental entity at a very early stage (e.g., the national population register might assign a national identification number at birth).

[1404] See also International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 9.

[1405] For an example see D. De Cock, B. Van Alsenoy, B. Preneel and J. Dumortier, "The Belgian eID Approach", *l.c.*, p. 123.

2.2 *AUTHORITATIVE SOURCE*

678. MAIN CHARACTERISTICS – In the context of identity management, corroboration of identity information typically involves consultation of one or more "authoritative sources".[1406] An authoritative source can be described as a repository of information which is recognized as being an accurate and up-to-date source of certain information within a particular context.[1407] An example of an authoritative source in the Belgian e-government would be the National Register, which is recognized as being the authoritative source for citizen attributes such as full name, gender, data of birth, official address, marital status, etc.[1408]

679. INFORMATION AS A STRATEGIC RESOURCE – In order to maximize administrative efficiency, several governments have introduced the principle of "single collection" into their e-government policies.[1409] This approach entails that the citizen's personal data is collected only once, and is later shared and re-used by other governmental entities.[1410] The designation of a repository as an authoritative source entails that this repository shall be considered the primary (and perhaps even "sole") source for the information within a particular context.[1411]

[1406] See e.g. D. Chadwick, "Federated Identity Management", in Alessandro Aldini, Gilles Barthe and Roberto Gorrieri (eds.), *Foundations of Security Analysis and Design V*, FOSAD 2007/2008/2009 Tutorial Lectures, Springer, 2009, p. 97-99.

[1407] See also J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), "Conceptual framework for identity management in e-government", *l.c.*, p. 45. In many documents authoritative sources are also referred to as "authentic sources" or "authentic registers" (see e.g. the European Commission Information Society and Media Directorate-General, E-government Unit, "A roadmap for a pan-European eIDM framework by 2010", l.c., p. 5. I have chosen to use of the term "authoritative" as it is more in line with identity management literature and because I believe the term "authoritative" better captures their actual role (it reflects the idea that they are seen as trustworthy within a certain context). Moreover, use of the term "authentic" may also in the long run engender confusion with concepts such as "authentication" or "data authenticity" in the way traditionally used in computer sciences.

[1408] D. De Cock, B. Van Alsenoy, B. Preneel and J. Dumortier, "The Belgian eID Approach", *l.c.*, p. 125-126

[1409] See e.g. J. Deprest and F. Robben, *eGovernment: the approach of the Belgian federal administration*, *o.c.*, p. 7. The EC eIDM Roadmap developed by the DG Information Society and Media of the European Commission also advocates single collection of personal data (European Commission, A Roadmap for a pan-European eIDM Framework by 2010, 2006, v1.0, Block VIII, available at http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf).

[1410] The use of authoritative sources is typically justified by the advantages of having single points of contact to update and manage information. Specifically, this approach helps to avoid the existence of multiple copies of the same information in different databases, among which discrepancies may start to develop over time. It is also said to increase convenience for citizens, as they will not be asked to provide the same information over and over again. See J. Deprest and F. Robben, eGovernment: the approach of the Belgian federal administration, *o.c.*, p. 6.

[1411] Verification against authoritative sources can take place at various stages of the life-cycle of an identity and can serve different purposes (during enrolment, authentication, authorization, etc.). The generic purpose is typically to confirm the validity of a certain proposition (e.g., an asserted attribute, the revocation status of a credential) in real time. (B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 21.)

680. RELATED PROCESSES – In principle, each item of data shall be subject to *proofing* and *verification* before being registered with an authoritative source.[1412] Once the data have been verified with an appropriate degree of assurance, the data shall be registered with the authoritative source. If not previously assigned, the authoritative source will assign one or more unique identifiers which can be used to identify and recognize the citizen in the future.

681. DATA FLOWS – Arrow (1) depicts the process of proofing and verification. Arrow (1) is bi-directional because the authoritative source may assign an identifier to the citizen (in case where it does not rely on a previously assigned identifier). A subset of data recorded by an authoritative source may be incorporated in a credential which is later issued to the citizen or verifier (see below).

2.3 CREDENTIAL SERVICE PROVIDER

682. MAIN CHARACTERISTICS – A credential service provider (CSP) is an entity that issues and/or manages credentials.[1413] Classic examples of credentials include passwords and digital signatures.[1414] In a narrow sense, the term "credential" refers only to data and does not include the hardware or software used to produce these data.[1415] However, CSPs may manage these aspects as well.[1416] For purposes of simplicity, this chapter does not further distinguish among the actors who might be involved in the creation and management of credentials.[1417]

[1412] For example, a citizen declaring a change of address might be required to present a photo ID at the moment of declaration. This declared change of address might subsequently be verified by a police officer visiting the citizen at his or her new home. In practice, the proofing and verification process may be conducted by a separate entity (sometimes referred to as the "Registration Authority").

[1413] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 2. A credential can be described as a set of data presented as evidence of a claimed identity and/or attribute. (*Id.*)

[1414] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 9 and 30.

[1415] Id. The term "credential" is thus used in very narrow sense here: it refers only to the data, not the token which incorporates the credential (e.g., the smart card containing the private key to generate a digital signature). See also Modinis project, Common Terminological Framework for Interoperable Electronic Identity Management, *l.c.*, p. 10.

[1416] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 9.

[1417] It is important to realize, however, that the credential management process may involve a plurality of actors. In case of the Belgian eID card, for example, the following actors are involved in the credential management process: (1) the municipalities, which act as the front-office registration and issuance authorities; (2) the National Register, which provides the necessary information for the creation of eID cards; (3) the card manufacturer (Zetes), who also acts as both the Card Initializer (CI) and the Card Personalizer (CP); (4) Certipost, who acts as the Certificate Authority (CA) and (5) Group 4 Securitor, which acts as a secure mail carrier for transportation of the eID cards and card request forms between the municipalities and the card manufacturer. (D. De Cock, B. Van Alsenoy, B. Preneel and J. Dumortier, "The Belgian eID Approach", *l.c.*, p. 126.) In this model, Zetes is the credential service provider *strictu sensu* as it generates the cryptographic key pairs which enable the eID card to create digital signatures. It also acts as the card manufacturer. However, the certificates corresponding to the public verification keys are issued by a separate entity, i.e. the Certificate Authority (Certipost). (*Ibid*, p. 129-130.)

683. RELATED PROCESSES – Credential management comprises all processes relevant to the lifecycle management of a credential or the means to produce credentials.[1418] It may involve some or all of the following processes: (1) creation; (2) issuance; (3) activation; (4) storage (5) revocation and/or destruction; (6) renewal and/or replacement and (7) record-keeping.[1419]

684. LEVELS OF ASSURANCE – Different credentials support different levels of entity authentication assurance.[1420] The Level of Assurance ("LoA") associated with a particular credential conveys the degree of confidence which a relying party may have that the identity (or other attribute) claimed by a particular entity in fact belongs to that entity.[1421] The type of credentials issued, as well as the safeguards that are implemented by the CSP, are key factors in determining which LoA will be reached during a particular authentication protocol.[1422]

685. DATA FLOWS – In principle, a CSP will only collect data emanating from an authoritative source (arrow (2)). Once a credential has been prepared, it can be issued to the citizen in question (arrow (3)). Arrow (3) is bi-directional as a citizen may notify the CSP that a credential should be revoked (e.g., in case of loss or theft). A verifier consults the CSP to request or confirm the validity of a credentials concerning a particular citizen (arrow (5)). As shown in Figure 2, the interaction between a CSP and a verifier can also be mediated by an integrator.

[1418] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 13 et seq.

[1419] *Id.*

[1420] Entity authentication assurance can be described as "degree of confidence reached in the authentication process that the entity is what it is, or is expected to be". International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 2.

[1421] In recent years, several initiatives have been undertaken in order to develop a common understanding and standardized approach to the issue of EAA. See e.g. W.E. Burr, D. F. Dodson and W.T. Polk, *Electronic Authentication Guideline*, NIST SP800-63, v1.0.2, available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf; Graux, H., Majava, J., "eID Interoperability for PEGS - Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms", *IDABC*, December 2007, available at http://ec.europa.eu/idabc/en/document/6484.html; Glade, B., *Identity assurance framework: Assurance Levels*, v2.0, 24 April 2010, Kantara Initiative, available at http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0; ISO/IEC, Information technology -- Security techniques -- Entity authentication assurance framework, *l.c.*, 36 p. and International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, 44 p. The overall approach of these initiatives is the following. They start by defining a number of assurance levels, typically four (e.g., "low", "moderate", "high" and "very high"). They then define the technical and organisational requirements which must be met in order to meet a certain level of assurance. This approach is designed to help decision-makers to assess what type of authentication mechanisms are appropriate for which applications, and whether or not reliance on a particular eID solution is suitable for their purposes. (B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 32).

[1422] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 12 et seq.

2.4 *INTEGRATOR*

686. MAIN CHARACTERISTICS – An integrator is an intermediary that facilitates interactions between entities that provide and consume identity-related services. Typical integrator services include (but are not limited to): (1) discovery; (2) orchestration; and (3) transformation.[1423] An example of an integrator in the Belgian e-government context would be the Crossroads Bank for Social Security (CBSS).[1424]

687. ROLE OF INTEGRATORS – Early on, e-Government architects realized that transforming resources and applications into functional products for end-users generally requires putting in place additional building blocks and services. Use of intermediaries or "integrators" was recommended to reduce the potential burden on individual service providers. The services offered by an integrator become part of a common framework, which could be then leveraged when developing applications.[1425] Section 5 will analyse two real-life examples of European e-Government integrators, namely the Internal Market Information (System) and the Pan-European Proxy Service (PEPS).

688. RELATED PROCESSES – In order to facilitate interactions between the providers and consumers of identity related services, an integrator must compile and maintain a directory of relevant resources (e.g., a list of trusted credential service providers). That way, when a verifier requests the attestation of identity information, the integrator will have at its disposal an overview of the sources from which a valid attestation might be obtained. Transformation involves the conversion of information from one format (e.g., the format of in which the attribute is provided by the CSP) to another format (e.g., the format the format understood by the verifier). Orchestration involves the strategic combination of resources to deliver a composite service (e.g., retrieval and verification of identity information from multiple sources to determine eligibility).[1426]

689. DATA FLOWS – As shown in Figure 2, integrators in principle only interact with credential service providers (CSP) and verifiers (arrow 5). As explained earlier, it is

---

[1423] X. Huysmans and B. Van Alsenoy (eds.), D1.3 Conceptual Framework – Annex I. Glossary of Terms, IDEM, v1.07, p. 20-21. See also J.C. Buitelaar, M. Meints, and B. Van Alsenoy (eds.), "Conceptual Framework for Identity Management in eGovernment", *l.c.*, p. 16.

[1424] For more information see the homepage of the Crossroadsbank of Social Security https://www.ksz-bcss.fgov.be. See also B. Van Alsenoy, "E-government Solutions: Trends and Developments in Belgian e-Government", in M. Meints and H. Zwingelberg (eds.), Identity Management Systems - recent developments", FIDIS Deliverable D3.17, 2009, p. 43, accessible at http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf (last accessed 15 November 2015).

[1425] B. Van Alsenoy, "E-government Solutions: Trends and Developments in Belgian e-Government", *l.c.*, p. 40.

[1426] For an example see B. Bruegger, *Reference Architecture*, FutureID deliverable D21.4, v1.1. 2014, p. 22 et seq, available at http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.04_WP21_v1.1_Reference%20Architecture.pdf (last accessed 18 January 2016).

perfectly possible for an entity to combine multiple roles. For example, an authoritative source might also act as a CSP, or a relying party might also act as a verifier. If that is the case, the integrator will obviously also interact with the authoritative sources and/or relying parties.

2.5 VERIFIER

690. MAIN CHARACTERISTICS – A verifier is an entity that corroborates identity information.[1427] A typical example of a verifier is an authentication service, which verifies the credentials presented by a citizen before he or she is granted access to a particular resource.[1428] An example of a verifier in the Belgian e-government context would be the Federal Authentication Service (FAS).[1429]

691. RELATED PROCESSES – When a citizen wishes to assert his identity (or other identity attributes) towards a relying party, the verifier will execute an authentication protocol designed to establish confidence in the asserted identity information.[1430] Authentication protocol requirements generally vary depending on the required Level of Assurance (LoA).[1431] For example, for a lower LoA, it may be sufficient for users to present a simple username-password combination. For higher LoAs, authentication may involve use of a cryptographic-based challenge-response protocols (which may in turn involve use of hardware tokens such as smart cards). Verification typically also involves checking the validity and/or revocation status of the presented credentials.

692. DATA FLOWS – Authentication services typically perform their functions at the moment where a citizen, holder of a digital identity, interacts with a relying party (e.g., to request access to a service). Arrow (4) depicts the request from the citizen to the relying party. Arrow (6) depicts the subsequent interaction between the citizen and verifier. Arrow (5) represents the communication between to the verifier and the CSP, which may (or may not) be mediated by an integrator. The communication between the verifier and the CSP generally serves to establish the validity and/or revocation status of the presented credentials. Arrow (7) depicts the request for authentication by the

---

[1427] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 10.

[1428] In principle, a verifier can be involved in multiple stages of entity authentication scheme and can perform both credential verification and/or identity information verification functions (International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 10). For purposes of conceptual clarity, the discussion here shall be limited to credential verification as part of an authentication protocol.

[1429] For more information visit http://www.fedict.belgium.be/en/identificatie_beveiliging/federal_authentication_service. See also B. Van Alsenoy, "E-government Solutions: Trends and Developments in Belgian e-Government", *l.c.*, p. 41.

[1430] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 16.

[1431] *Id.*

relying party, as well as the subsequent response by the verifier regarding the outcome of the authentication process.

2.6 RELYING PARTY

693. MAIN CHARACTERISTICS – A relying party is an entity that relies on identity information.[1432] The identity information may be relied on for a variety of purposes, such as account management, access control, authorization decisions, etc.[1433] An example of a relying party in the context of Belgian e-Government is the Tax-on-Web application, a service operated by the Ministry of Finance which enables citizens to submit their tax returns online.[1434]

694. RELATED PROCESSES – A relying party can itself perform the operations necessary to retrieve and authenticate identity information, or it may entrust these operations to a third party (verifier).[1435]

695. DATA FLOWS – Arrow (4) depicts the interaction between the citizen and relying party. Arrow (7) depicts the interaction between the relying party and verifier who has been requested by relying party to authenticate the citizen on its behalf.

3 ROLES

696. PROCESSING PURSUANT TO A LEGAL BASIS – In an e-government setting, any participant (authoritative source, credential service provider, integrator, …) might be acting as a controller, processor or third party depending on the application at hand.[1436] When a legal provision mandates a certain form of processing, it should in principle indicate which entity shall act as a controller. Where legislators are not explicit in this regard, but merely entrusts the processing to a particular body, it may be assumed that the latter will be responsible for the processing operations it performs pursuant to this legal basis.[1437]

[1432] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 9.
[1433] *Id.*
[1434] For more information see www.taxonweb.be
[1435] International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, *l.c.*, p. 9
[1436] J.C., Buitelaar, M. Meints and E. Kindt, "Towards requirements for privacy-friendly identity management in eGovernment", *l.c.*, p. 16.
[1437] D. De Bot, *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, *o.c.,* p. 35. See also *supra*; nr. 167.

697. APPLICATION OF GENERAL CRITERIA – While the legal basis which authorizes the processing may provide clarity, there will still be situations where it is difficult to determine whether a governmental entity is acting as a controller or processor. For instance, several governmental entities might be charged with complementary tasks of public interest. This, in turn, might require multiple governmental entities, each within their respective domain, to carry out certain processing operations. If there is no clear specification in the law as to which entity shall act as a controller, their respective roles are determined by the general criteria of the Directive (purposes, means).[1438]

698. OUTLINE – The aim of this section is to investigate the potential roles of the actors identified in the previous section, using the general criteria of Directive 95/46. This exercise is by no means superfluous, as similar configurations arise in private sector identity management applications. At a practical level, it remains necessary to analyse the specific practices within a particular identity management system in order to determine the responsibilities of each actor involved.[1439] The analysis provided in the following sections is therefore of a high-level nature. Section 5 will go more in-depth by analysing two practical examples. Section 5.1 shall describe how the allocation of roles and responsibilities was addressed in the context of the Internal Market Information (IMI) system. Section 5.2 will explore the guidance provided by a subgroup of the Article 29 Working Party in relation to the Pan-European Proxy Service (PEPS).

3.1 CITIZEN

699. HIGH LEVEL ANALYSIS – Identity information about citizens typically relates to an identified or identifiable individual.[1440] As a result, citizens shall generally qualify as "data subjects" rather than as "controllers" or "processors".

700. CITIZENS IN "CONTROL" OF THEIR OWN DATA? – Certain identity management applications enable citizens to exercise control over the disclosure of identity information. This raises the question as to whether or not citizens might be considered as (co-)controllers towards the processing of their own personal data. There are essentially two arguments which can be made against such a proposition. First, this interpretation cannot be reconciled with the regulatory scheme of Directive 95/46/EC. This scheme is predicated on the notion that the data controller is an entity other than the data subject him- or herself. An individual person might act as a controller of

[1438] Cf. *supra*; nr. 168.
[1439] T. Olsen, and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *l.c.*, p. 420.
[1440] Legal persons and other entities (e.g., association of fact) may also be holders of digital identity in an e-Government context. In order to engage in online transactions, however, they must be represented by a natural person acting as an agent on their behalf. While legal persons do not qualify as data subjects, their legal representatives do. Moreover, in certain instances, the name of a legal person may also identify a natural person, in which case it may constitute personal data.

personal data relating to others[1441], but not of his or her own personal data. Accepting that the data subject could act as a controller of the processing of his own personal data would have rather absurd implications: the data subject would have to obtain consent from him- or herself, provide him- or herself with notice, etc.[1442] Second, the fact that the data subject authorizes the disclosure of personal information within a certain context merely signifies his or her agreement towards processing. It does not exclude the presence of another entity who determines the "purposes and means" for the processing of these data. Even where the individual has the ability to "control" the release of his or her personal data (and might even decide the medium that is used), this does not alter the role of the collectors or handlers of the individual's data.

3.2 AUTHORITATIVE SOURCE

701. HIGH LEVEL ANALYSIS – Storage of personal data by an authoritative source typically results from a business activity (in case of private actors) or public mission (in case of public actors). Sometimes, the storage of personal data is the primary activity of the authoritative source. The Belgian National Register, for example, has as its main public mission to collect, record and make available certain types of information regarding the inhabitants of Belgium.[1443] In other cases, storage of information by authoritative sources is a by-product of other activities. For example, a hospital patient registry may act as an authoritative source attesting to the existence of a patient-doctor relationship.[1444] Authoritative sources must in principle be considered as "controllers" within the meaning of article 2(d), as they determine the purposes and means of their

---

[1441] See the Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596. See also B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 69-70; Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", WP163, 12 June 2009, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf; European Network and Information Security Agency (ENISA), "Online as soon as it happens", February 2010, p. 33-34, available at http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens.

[1442] Alternatively, one could argue that such processing would be exempted from the application of the Directive under art. 3(2) (exemption of processing carried out in the course of a purely personal or household activity) (see references in previous footnote). However, this finding would not undercut the argument that the allocation of responsibilities under the Directive is structured implies that the data subject and the controller are separate entities.

[1443] See article 1 and 2 of the Law of 8 August 1983 organising a register of natural persons (B.S., 21 March 1984).

[1444] For more information see Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL), Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, Afdeling «Gezondheid», Beraadslaging nr. 11/088 van 18 oktober 2011, gewijzigd op 9 juni 2015, met betrekking tot de nota betreffende de elektronische bewijsmiddelen van een therapeutische relatie en van een zorgrelatie, SCSZG/15/088, 9 June 2015, accessible at https://www.privacycommission.be/sites/privacycommission/files/documents/beraadslaging_AG_088_2011.pdf. See also Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL), Aanbeveling nr 09/2012 van 23 mei 2012 uit eigen beweging in verband met authentieke gegevensbronnen in de overheidssector (CO-AR-2010-005), accessible at https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_09_2012_0.pdf (last accessed 16 November 2015).

own processing activities (or have been explicitly entrusted by law to conduct such processing).

702. SCOPE OF CONTROL – The control exercised by an authoritative source extends to all their own processing operations, including acts of disclosure to third parties. The authoritative source in principle does not control any of the subsequent processing operations undertaken by CSPs, integrators, verifiers or relying parties. After all, the purposes pursued by an authoritative source in keeping the data shall in principle be distinct from the specific purposes pursued by the entities to whom the personal data is disclosed. The act of disclosure itself, however, is attributable to the authoritative source. As a result, the authoritative source should only agree to make the information available once it has obtained sufficient assurance of the compatibility and/or legitimacy of the processing which the recipient purports to undertake.[1445]

3.3 CREDENTIAL SERVICE PROVIDER

703. HIGH LEVEL ANALYSIS – A credential service provider shall generally be considered a controller within the meaning of article 2(d). While it cannot be excluded that an entity operates a credential service "on behalf of" another entity, credential services are often dedicated services designed and controlled by the entity which provides them.[1446]

704. SCOPE OF CONTROL – A credential service provider shall in principle act as a controller in relation to the collection, adaption, storage and transmission of identity information necessary to deliver the credential service. Its control in principle does not extend to any of the subsequent processing operations undertaken by integrators, verifiers or relying parties.

705. STANDARDISATION – While credential service providers decide for themselves how to provide their services, they will often make use of existing standards. Identity management standards and specifications have been developed by a variety of standardisation bodies, including ISO, ITU-T, ETSI and Liberty Alliance.[1447] The Liberty Alliance protocol for identity federation and single sign-on was studied by the Article 29 Working Party as part of its Working Document on on-line authentication services.[1448]

[1445] See also B. Van Alsenoy, N. Vandezande, K. Janssen, a.o., "Legal Provisions for Deploying INDI services", *l.c.*, p. 25.

[1446] See also Article 29 Data Protection Working Party, "Working Document on on-line authentication services", WP 68, 29 January 2003, p. 14 (considers Microsoft as "data controller" in relation to .NET passport, which is an entity which combines the role of CSP and verifier).

[1447] See also *supra*; at footnote 1421.

[1448] Article 29 Data Protection Working Party, "Working Document on on-line authentication services", *l.c.*, p. 11-13. Single sign-on is understood as the ability of the consumer to, after having authenticated once with a particular Identity Provider, to interact with various Service Providers within a "Circle of Trust" (CoT) without needing to re-authenticate. Any time a user account has been federated among Service

The Working Party considered the Liberty Alliance protocol to be "neutral" from a data protection perspective.[1449] It allows compliance with the Directive but does not require it. As far as the obligation to comply with the Directive is concerned, the Working Party made the following observations[1450]:

- the Liberty Alliance is responsible as far as the technical development of the project is concerned;
- each service provider that implements Liberty specifications bears the responsibility of complying with data protection legislation when operating its "Liberty-enabled" web services;
- service providers within a Circle of Trust become data controllers at the time users visit their websites;
- the different participants should have clear contractual agreements in which the obligations of each party concerning data protection aspects are made explicit.[1451]

706. ASSSESMENT – Even though the Liberty Alliance single sign on protocol was considered to be "neutral" from a data protection perspective, the Working Party stated that the Liberty Alliance should make sure that their specifications allow the organisations that implement and use them to comply with the Directive. The Working Party additionally encouraged them to develop recommendations and guidelines that motivate companies to use the technical specifications in a privacy-compliant or even privacy-enhancing manner. It is unclear, however, on which ground such responsibility is based.[1452] Even if designers take data protection issues into consideration when developing technical specifications, it is primarily the organisations that implement these specifications that shall be responsible for compliance with data protection legislation.[1453]

3.4 INTEGRATOR

707. HIGH LEVEL ANALYSIS – The legal status of integrators can be difficult to determine. By definition, an integrator acts as an intermediary. As a result, the integrator may present itself to some as a processor, who merely facilitates the exchange of information on behalf of others. Others might see integrators as controllers, especially

---

Providers; the Service Provider managing the federated account will be able to act as an authentication service towards other Service Providers who are part of the same Circle of Trust.

[1449] *Ibid*, p. 12.

[1450] *Ibid*, p. 12 and p. 14-15.

[1451] See also J. Alhadeff and B. Van Alsenoy (eds.), "D6.2 Contractual framework", *l.c.*, p. 38-39

[1452] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *l.c.*, p. 418. Of course, if the developed protocols were to impede compliance this could significantly discourage organisations from implementing those specifications.

[1453] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *l.c.*, p. 418.

if they act autonomously in the development and provisioning of their services. Finally, it is also possible that the integrator determines the purposes and means of its processing in conjunction with others. A useful parallel might be drawn to the SWIFT case, which involved a financial messaging service that combined both controller and processor characteristics.

708. SWIFT – The Society for Worldwide Interbank Financial Telecommunication ("SWIFT") is a worldwide financial messaging service which facilitates international money transfers. SWIFT was organized in 1973 by a group of European banks that wanted to develop a new method to send payment instructions to correspondent banks in a standardised manner.[1454] Later, SWIFT expanded its service catalogue and began offering its services to other types of financial institutions. Despite the fact that SWIFT had always considered itself to be a mere processor of the instructing financial institutions, the Article 29 Working Party held that SWIFT acted as a data controller.[1455] The main reasons advanced to support this conclusion were that[1456]:

- SWIFT does more than just act on behalf of its clients. It has taken on specific responsibilities which, by their nature and scope, go beyond the usual set of instructions and duties incumbent on a processor;
- The management of SWIFT operates in the context of a formal cooperative network which determines both the purposes and means of data processing within the SWIFTNet service;
- SWIFT management decides what personal data is processed via that service, and the level of information that is provided to financial institutions in relation to the processing;

[1454] Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", WP128, 22 November 2006, 10, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf. The SWIFT Opinion had been preceded by an investigation conducted by the Belgian Data Protection authority: see Commissie voor de Persoonlijke Levenssfeer, Advies Nr 37/2006 van 27 september 2006 betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC), available at https://www.privacycommission.be/sites/privacycommission/files/documents/advies_37_2006_1.pdf. See also the subsequent opinion adopted by the CBPL in 2008: Commissie voor de Persoonlijke Levenssfeer, Decision of 9 December 2008 regarding the Control and recommendation procedure initiated with respect to the company SWIFT, 75p. available at https://www.privacycommission.be/sites/privacycommission/files/documents/swift_decision_en_09_12_2008.pdf (last accessed 26 April 2016).

[1455] Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", *l.c.*, 11. For a more detailed discussion of the factual background to the SWIFT case see G.G. Fuster, P. De Hert and S. Gutwirth, "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology* 2008, Vol. 22, p. 191–202.

[1456] Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", *l.c.*, 11. See also B. C. Treacy, "Lessons from SWIFT: the 'controller' v 'processor' dilemma", Complinet 2008, p. 2 available at https://www.hunton.com/files/Publication/38eae420-4098-4082-aba8-ce1cdbc14d3d/Presentation/PublicationAttachment/83cddb21-a689-4179-a0b5-0e4d10e0df88/Treacy_SWIFT_1.08.pdf (last accessed 26 April 2016).

- SWIFT management is able to determine the purposes and means of processing by developing, marketing and changing the existing or new SWIFT services (e.g., by determining the standards applicable to its clients as to the form and content of payment orders without requiring their prior consent);
- SWIFT provides added value to the processing, such as the storage and validation of personal data and the protection of personal data with a high security standard;
- SWIFT management had the autonomy to take critical decisions in respect to the processing, such as determining the security standard to be applied to the data and the location of its operating centers;
- SWIFT management negotiates and terminates with full autonomy its services agreements and drafts and changes its various contractual documents and policies.

While acknowledging that some elements suggest that SWIFT may have acted as a processor in the past, the Article 29 Working party considered that the effective margin of maneuver possessed by SWIFT management precluded its qualification as a mere processor. On the other hand, SWIFT was not considered to be as acting as the sole controller.[1457] Rather, there existed a joint responsibility among the financial institutions and the SWIFT cooperative for the processing of personal data via the SWIFTNet FIN service.[1458]

709. ASSESSMENT – The SWIFT case illustrates the "hybrid" status of integrators, who can display characteristics of both controllers and processors. In the end, it seems that the qualification of an integrator as either controller or processor will depend on which characteristics are perceived as dominant: factual influence over the processing or the auxiliary nature of the service provided.

3.5 VERIFIER

710. HIGH LEVEL ANALYSIS – An investigation into the legal status of verifiers presents similar issues as the analysis of integrators. Because identity verification is an auxiliary function, performed in support of some other activity, verifiers can easily be viewed as processors. After all, verifiers processes personal data "on behalf of" relying

[1457] Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", *l.c.*, 12

[1458] The level responsibility was not considered to the same among all the participants. In particular, the Article 29 Working Party argued that: "*[…] joint responsibility does not necessarily mean equal responsibility. Whilst SWIFT bears primary responsibility for the processing of personal data in the SWIFTNet FIN service, financial institutions also bear some responsibility for the processing of their clients' personal data in the service*". (*Ibid*, 13) (emphasis added). Similarly, in its executive summary the Working Party indicated that "*Both SWIFT and instructing financial institutions share joint responsibility, although in different degrees, for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Directive.*"

parties or credential service providers. On the other hand, certain verification services may be sufficiently independent and autonomous, thereby justifying the qualification as "controller". The Pan-European Proxy Service (PEPS) illustrates the conceptual difficulties that may arise in determining the appropriate qualification of verifiers.[1459]

3.6 RELYING PARTY

711. HIGH LEVEL ANALYSIS – A relying party in principle acts as a controller in relation to its own processing operations. Once the identity information has been verified, the party will proceed to process the data for its own purposes. Each relying party therefore has its own responsibility to comply with data protection legislation.[1460]

712. SCOPE OF CONTROL – The scope of control exercised by a relying party extends not only to its own processing operation, but also to its decision to make use of the services provided by credential service providers, integrators and/or verifiers. Even in cases where a relying party has limited options, it shall in principle be obliged to assess the possible implications and privacy risks to data subjects when they make use of such services.

4 ALLOCATION OF RESPONSIBILITY AND RISK

713. LEGAL QUALIFICATION – According to Olsen and Mahler, most identity management systems consist of "multiple collaborating but single controllers".[1461] The previous section confirmed that several entities indeed act as controllers towards their own processing operations. Nevertheless, it cannot be excluded certain entities assume the role of processor, nor can it be excluded that that several entities jointly determine the purposes and means of a particular processing operation.[1462]

714. MUTUAL DEPENDENCE – Co-controllers and collaborating single controllers enjoy considerable flexibility in determining how to achieve compliance.[1463] Under Directive 95/46, they are not formally obliged to put in place an arrangement through

---

[1459] Cf. *infra*; nrs. 759 et seq.

[1460] See also Article 29 Data Protection Working Party, "Working Document on on-line authentication services", *l.c.*, p. 9 ("*It should be clarified in any case that, apart from of the role that Microsoft plays within the .NET Passport system, all participating sites are to be considered as data controllers in respect of their own processing operations. They have therefore their own responsibility to comply with privacy legislation.*")

[1461] T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *l.c.*, p. 420.

[1462] See also S. Deadman (ed.), *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*, Liberty Alliance Project, February 23, 2005, p. 15-16.

[1463] Cf. *supra*; nr. 116.

which they mutually allocate responsibilities.[1464] The incentive to put in place an appropriate arrangement must therefore come from elsewhere. One possible incentive is the fact that the collaborating single controllers and co-controllers may be dependent on one and other to ensure compliance with their own obligations.[1465] Still, there may be situations where controllers do not feel obliged to engage with other controllers in ensuring compliance ("every controller for himself"). Such an outcome is likely to have a negative impact on data subjects, who then face the burden of finding out which controller is responsible for which specific aspect of the processing.

715. RESPONSIBILITIES TO BE ALLOCATED - There are many responsibilities which need to be allocated within an e-government framework in order to ensure compliance with both legal and policy requirements. The following is by no means an exhaustive list of several of the tasks and responsibilities which will most likely need to be considered[1466]:

- which entities shall act as act as authoritative sources for which data sets;
- which entities shall perform which authentications, authorizations and checks;
- which entities will be charged with the maintenance of logs for which operations;
- which entities will be charged with the updating of technical policies;
- which entities shall serve as a front-office to accommodate the rights of data subjects such as the right of access and correction;
- which entities shall serve as a point-of-contact in the event of a security breach; and
- which entities shall be charged with periodic verification of compliance (audit).

716. ROLE OF LEGISLATION AND POLICY – The development of e-government applications does not happen overnight. It requires careful planning and co-ordination, as well as a clear vision for the future. Legislation and policy play a key role in securing the participation and of all relevant actors. It should also play a key role in defining and delineating the data protection responsibilities of the actors involved. The following section will analyse how the European Commission, and eventually the European legislature, approached this issue in the context of the Internal Market Information System.

[1464] See also T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *l.c.*, p. 421 (questioning the legal basis for the advice issued by the WP29).

[1465] For example, a relying party can only fulfil its obligation to maintain data accuracy if the data maintained by authoritative sources is sufficiently accurate. In a high-risk setting (e.g. access to medical records), the relying party would expose itself to liability if it did not obtain adequate assurances as to the reliability of the information it relies on. Conversely, the authoritative source requires appropriate assurance that personal data is being disclosed to an authorized entity, lest it violate its duty to ensure confidentiality and security of processing.

[1466] J.C. Buitelaar, M. Meints and E. Kindt, "Towards requirements for privacy-friendly identity management in eGovernment", *l.c.*, p. 17.

5 PRACTICAL EXAMPLES

5.1 INTERNAL MARKET INFORMATION SYSTEM

A. Introduction

717. WHAT IS IMI? – The Internal Market Information (IMI) system is an ICT tool provided by the European Commission designed to facilitate information exchange among Member States. In particular, IMI aims at providing support for the practical implementation of Union acts that require an exchange of personal data between Member States' administrations or between Member States and the Commission.[1467] Currently, the use of IMI is limited to the implementation of Union acts in the field of the internal market, which are listed in the Annex to the IMI Regulation 1024/2012.[1468]

718. ORIGIN AND DEVELOPMENT – The IMI project officially started in 2005 in the context of the IDABC program.[1469] IMI was initially built to support one-to-one communication between competent authorities in the implementation of the Professional Qualification Directive and the Services Directive.[1470] Over time, the system was gradually expanded to support other areas of administrative co-operation and to provide additional functionalities (e.g., one-to-many workflows, repository services).[1471] In 2007, the Article 29 Working Party issued a first Opinion regarding data protection issues related to the IMI System. Shortly thereafter, the Commission published a Decision concerning the implementation of the IMI system as regards the protection of personal data.[1472] The Decision was followed by an Opinion of the European Data Protection Supervisor, which outlined additional steps to be taken.[1473] In 2009, the Commission issued a Recommendation containing data protection guidelines for the IMI

[1467] Article 3(1) of Regulation No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal market Information system and repealing Commission Decision 2008/49/EC, *O.J.* 14 November 2012, L 316/1-11. See also recitals (1) and (2)
[1468] Such as Directive 2005/36/EC, L 255/22-142.
[1469] See article (4) and also http://ec.europa.eu/idabc/en/document/5378/5637 (last accessed 22 July 2009).
[1470] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI') 22 November 2011, p. 2 accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-11-22_IMI_Opinion_EN.pdf (last accessed 18 November 2015).
[1471] Id.
[1472] European Commission, Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *O.J.* 16 January 2008, L 13/18.
[1473] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01), *O.J.* 25 October 2008, C 270/1.

system.[1474] In 2012, the European and the Council repealed Commission Decision 2008/49/EC by way of Regulation 1024/2012 on administrative cooperation through the Internal Market Information System ("the IMI Regulation").[1475]

B. Functionalities

719. STRUCTURED INFORMATION EXCHANGE – In essence, the IMI system acts as a closed network which allows the "competent authority" of a particular Member State to identify its counterpart in another Member State and to exchange information using the IMI network.[1476] In addition to its search function, IMI provides users with a set of pre-translated menus, as well as standardised questions and procedures to support the information exchange. IMI now also supports one-to-many workflows (e.g., alert mechanisms, notifications) and repository services. All functionalities of IMI are accessible via web pages.[1477]

720. EXAMPLE – One of the first IMI functionalities was to assist competent authorities in determining the authenticity of credentials presented by an EU citizen

[1474] European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), 2009/329/EC, *O.J.* 18 April 2009, L 100/17.
[1475] Regulation No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC, *O.J.* 14 November 2012, L 316/1-11. Initially, the European Commission relied primarily upon Decision 2004/387/EC (the "IDABC" decision) in combination with the Professional Qualifications Directive and the Services as justification for the processing of personal data within IMI. Both the Article 29 Working Party and the EDPS expressed multiple reservations as to the adequacy of these instruments towards ensuring the legitimacy of processing. (See in particular Article 29 Data Protection Working Party, "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", WP 140, 20 September 2007, p. 8-10 and European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01)", *l.c.*, paragraphs 12-28.) In its opinion of 2007, the Article 29 Working Party recommended that the Commission adopt an "ad hoc" solution to support the existing legal basis in the form of a Commission Implementing Decision. Decision 2008/49/EC "concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data" was adopted in response to this recommendation. Despite this measure, the EDPS has continued to express its reservations as to the presence of a sufficient legal basis, particularly in relation to the requirements that such legal basis must be sufficiently clear and specific, and provide a sufficient degree of legal certainty. European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01)", *l.c.*, paragraphs 18 et seq. It was not until 2012 that IMI was provided a solid and independent legal basis by way of Regulation 1024/2012. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", 22 November 2011. p. 2-3
[1475] Such as Directive 2005/36/EC, L 255/22-142.
[1476] See also recital (2) of Regulation No 1024/2012
[1477] See Article 29 Data Protection Working Party, "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", *l.c.*, p. 4.

from a different Member State. The 2009 Commission Data Protection Guidelines contain an illustrative example:

> "*A German doctor resident in Berlin marries a French man and decides to start a new life in Paris. The German doctor wants to practice her profession in France and therefore submits titles and diplomas to the Order of Doctors in France. The person dealing with the file has doubts about the authenticity of one of the diplomas and uses IMI to check with the competent authority in Berlin.*" [1478]

721. A FEDERATION OF AUTHORITATIVE SOURCES – The IMI network can be seen as a "federation" of authoritative sources for specific attributes.[1479] The IMI system itself thereby acts as an integrator.[1480] It provides a platform through which a relying party (receiving country) may request corroboration of a particular attribute (prerequisite qualification) with the relevant competent authority (authoritative source) in another Member State (country of origin). Upon receipt of a request through IMI, the relevant competent authority will query its own databases in order to return the appropriate response.

C. Actors

722. OUTLINE - The three main actors involved in the administration of the IMI system are (1) the European Commission; (2) the IMI coordinators; and (3) the competent authorities. Jointly they are referred to as the "IMI actors".[1481] The term "IMI user" is used to refer to natural persons working under the authority of an IMI actor.[1482]

723. EUROPEAN COMMISSION – The European Commission hosts and maintains the IMI system in a data centre in Luxembourg.[1483] The Commission also provides the software for IMI, manages the network of national IMI co-ordinators and is involved in the training of and technical assistance to IMI users.[1484] The European Commission can also lay down practical arrangements to facilitate the efficient exchange of information

---

[1478] European Commission, European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), *l.c.,* p. 28.
[1479] One should note, however, that IMI currently does not incorporate national eIDM products in any way: IMI users are provided with credentials (username/passwords/roles) through their national co-ordinators and local administrators. In this sense the IMI model differs from "classic" identity federation models, whereby the mutual reliance on various identity providers is a key aspect. Though managed in a distributed fashion, there is in fact a "centralised" rather than federated IdP model for IMI (only authoritative sources are "federated").
[1480] Compare *supra*; nrs. 686 et seq.
[1481] Article 5(g) of Regulation No 1024/2012.
[1482] Article 5(h) of Regulation No 1024/2012.
[1483] European Commission, *The Internal Market Information (IMI) System User Handbook*, Update 2012, Publications Office of the European Union, Luxembourg, 2012, p. 8, available at http://ec.europa.eu/internal_market/imi-net/_docs/library/user_handbook_en.pdf (last accessed 17 November 2015).
[1484] Recital (9) of Regulation No 1024/2012.

through IMI by way of implementing acts.[1485] The Commission does not participate in administrative cooperation procedures involving the processing of personal data, except where required by the provision of a Union Act listed in the Annex of Regulation No 1024/2012.[1486]

724. IMI COORDINATOR – An IMI coordinator is a body appointed by a Member States to perform support tasks necessary for the efficient functioning of IMI.[1487] Relevant support tasks include registration of competent authorities, acting as a contact point for IMI actors of the Member State and providing knowledge, training and assistance to IMI actors of that Member State.[1488] Each Member state has one National IMI Co-ordinator ("NIMIC"). At the discretion of the Member State, Delegated IMI Coordinators ("DIMICs") may be appointed to take over some or all coordination responsibilities, for example in relation to a particular legislative area or geographical region.[1489]

725. COMPETENT AUTHORITY – A competent authority is any body which carries responsibilities relating to the application of national law or Union acts in one or more internal market areas.[1490] The competent authorities are the ones actually using the IMI system to exchange information relevant to the performance of their duties. Competent authorities that collaborate through IMI are obliged to provide an adequate response within the shortest possible period of time, in accordance with the applicable Union act.[1491]

D. Roles

726. COMMISSION DECISION 2008/49/EC - The first effort towards defining the roles and responsibilities of the actors involved in IMI was made in Commission Decision 2008/49/EC.[1492] Article 3, first indent of the Decision simply provided that

> "*The responsibilities of the controller under Article 2(d) of Directive 95/46/EC and Article 2(d) of Regulation (EC) No 45/2001 shall be jointly exercised by the IMI actors pursuant to Article 6 in accordance with their respective responsibilities within IMI*".

[1485] Recital (27) of Regulation No 1024/2012.
[1486] Article 8(3) of Regulation No 1024/2012.
[1487] Article 5(e) of Regulation No 1024/2012.
[1488] See article 6 of Regulation No 1024/2012.
[1489] European Commission, *The Internal Market Information (IMI) System User Handbook*, Update 2012, Publications Office of the European Union, Luxembourg, 2012, p. 8, available at http://ec.europa.eu/internal_market/imi-net/_docs/library/user_handbook_en.pdf (last accessed 17 November 2015)
[1490] Article 5(f)) of Regulation No 1024/2012.
[1491] Article 7(1) of Regulation No 1024/2012.
[1492] See European Commission, Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *O.J.* 16 January 2008, L 13/18-23.

The European Data Protection Supervisor (EDPS), however, considered that the allocation of responsibilities in article 3 was "unclear and ambiguous".[1493] The EDPS recommended that at least the following specifications be added:

- "*each Competent Authority and IMI coordinator is a controller with respect to its own data processing activities as a user of the system;*
- *the Commission is not a user, but the operator of the system, and it is responsible, first and foremost, for the technical operation, maintenance, and ensuring the overall security of the system, and that*
- *the IMI actors share responsibilities with respect to notice provision, and provision of right of access, objections, and rectifications […]".* [1494]

The EDPS then proceeded to outline the ways in which the IMI actors might provide notice to data subjects and accommodate data subject rights. It is worth noting, however, that the EDPS did not formally label the European Commission as either a "controller" or "processor". While the role of competent authorities and IMI coordinators as controllers was made explicit, the Commission received the ambiguous label of "operator".

727. COMMISSION RECOMMENDATION 2009/329/EC – Following the Opinion of the EDPS, the European Commission issued a Recommendation on data protection guidelines for IMI.[1495] With the recommendation, the Commission sough to give interim effect to the EDPS' recommendations. Regarding the legal qualifications of the actors concerned, the Commission noted that

> "*IMI is a clear example of joint processing operations and joint controllership. For example, whilst only the competent authorities in the Member States exchange personal data, the storage of these data on its servers is the responsibility of the European Commission. Whilst the European Commission is not allowed to see this personal data it is the operator of the system who physically processes the deletion and rectification of the data*."[1496]

728. REGULATION 1024/2012 – Article 6(4) of Regulation 1024/2012 confirms that each IMI coordinator shall be considered a controller "*with respect to its own data processing activities as an IMI actor*". Article 7(3) likewise provides that each competent authority shall be a controller with respect to the data processing activities of IMI users acting under its authority. Once again, the European Commission is labelled neither "controller" nor "processor". Article 8 simply lists the responsibilities of the Commission

[1493] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01)", *l.c.*, paragraph 34.
[1494] *Ibid*, paragraph 35.
[1495] European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), 2009/329/EC, *O.J.* 18 April 2009, L 100/17.
[1496] *Ibid*, p. 17.

(e.g., ensuring security, operating a helpdesk, etc.), without specifying the Commission's legal status. Only the EDPS, in his Opinion of 22 November 2011 clearly stated that the European Commission should also be considered a "controller".[1497] The label was not carried over, however, to the text of Regulation 1024/2012.

729. ASSESSMENT – In contrast to Commission Recommendation 2009/329/EC and the EDPS Opinion of 2007, Regulation 1024/2012 does not refer to joint controllership. Instead, it emphasises that IMI co-ordinators and competent authorities are each considered to act as controller "*with respect to their own data processing activities*". Such language is indicative of a relationship among collaborating single controllers, rather than a relationship among joint controllers. Regulation 1024/2012 does not clearly specify whether the European Commission is acting as a controller or not. Nevertheless, it seems clear that the Commission is acting also acting a controller in relation to its own processing activities within the IMI system (and possibly as a partial joint controller in relation to certain activities undertaken by the Member States).[1498]

E. Responsibilities

730. OUTLINE – Regulation 1024/2012 lays down the basic rules for the use of the IMI system and specifies the main functions and responsibilities of the actors involved in IMI. It also contains several provisions addressing data protection requirements, such as confidentiality[1499], purpose limitation[1500], retention of data[1501], special categories of data[1502], security[1503], transparency[1504], and data subject rights[1505]. The following paragraphs will analyse the allocation of responsibilities among IMI actors.

i. Confidentiality and security

731. EUROPEAN COMMISSION – Regulation 1024/2012 assigns the European Commission primary responsibility for ensuring the security of the IMI system.[1506]

[1497] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", *l.c.*, paragraph 34.
[1498] The IMI privacy statement of the European Commission takes the view that the collection and viewing, of personal data of persons who are the subject of an information falls under the sole responsibility of the Member States. See p. 1 of http://ec.europa.eu/internal_market/imi-net/_docs/data_protection/privacy_statement_en.pdf (last accessed 25 November). This suggests that the Commission also views its relationship with the Member States as one of separate controllers.
[1499] Article 10 of Regulation No 1024/2012.
[1500] Article 13 of Regulation No 1024/2012.
[1501] Article 14 of Regulation No 1024/2012.
[1502] Article 16 of Regulation No 1024/2012.
[1503] Article 17 of Regulation No 1024/2012.
[1504] Article 18 of Regulation No 1024/2012.
[1505] Article 19 of Regulation No 1024/2012.
[1506] See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", *l.c.*, paragraph 65.

Article 17(2) provides that the Commission must put in place the necessary measures to ensure security of personal data processed in IMI, including appropriate access control mechanisms and a security plan which shall be kept up-to-date.[1507] The Commission must also ensure that, in the event of a security incident, it is possible to verify what personal data have been processed in IMI, when, by whom and for what purpose (article 17(3)).

732. OTHER IMI ACTORS – While the Commission is responsible for a predominant part of the security of IMI, the other IMI actors (i.e., the IMI coordinators and the competent authorities) remain obliged to take the necessary procedural and organisational measures to security of personal data processed by them in IMI (article 17(4)). Binding IMI users to appropriate confidentiality obligations and limiting the access rights of individual IMI users are examples of measures which other IMI actors can take to help ensure the confidentiality and security of personal data processed by them in IMI.[1508]

733. ASSESSMENT – Given that the Commission provides and manages the software and IT infrastructure for IMI, it seems logical that the Commission carries the primary responsibility for ensuring the overall security of the IMI system. Nevertheless, the behaviour of other actors participating in IMI can impact the confidentiality and security of personal data processed within IMI. Moreover, as data controllers, each actor participating retains its own security obligation for information under its control. It is therefore logical that they remain responsible for the security of personal data "processed by them" in IMI.[1509]

[1507] See also article 9(4): "*appropriate means shall be put in place by the Commission and the Member States to ensure that IMI users are allowed to access personal data processed in IMI only on a need-to-know basis and within the internal market area or areas for which they were granted access rights*". IMI uses system of delegated administration to manage access rights. The National IMI Co-ordinators are responsible for ensuring that the relevant competent authorities are registered in IMI and can access (only) the modules correspond to their area of competence. Each competent authority is in turn obliged to appropriately manage the access rights of the IMI users under its authority. See European Commission, *Managing access to IMI*, not dated, p. 2, accessible at http://ec.europa.eu/internal_market/imi-net/_docs/training/managing_access_en.pdf. See also European Commission, *IMI roles and responsibilities*, not dated, accessible at http://ec.europa.eu/internal_market/imi-net/_docs/training/roles_responsibilities_en.pdf and European Commission, *Managing my authority and users*, not dated, accessible at http://ec.europa.eu/internal_market/imi-net/_docs/training/managing_authority_users_en.pdf (last accessed 25 November 2015).

[1508] See article 10 of Regulation 1024/2012. See also European Commission, "Data protection guidelines for IMI users", *l.c.*, p. 5-6.

[1509] See also Principle 2 of the OECD Recommendation on Digital Security Risk Management, which stipulates that all stakeholders should take responsibility for the management of digital security risks "*based on their roles, the context and their ability to act*". (OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2015, accessible at http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf)

ii. Data quality

734. EUROPEAN COMMISSION – IMI is based on pre-defined workflows ("administrative cooperation procedures") which allow IMI actors to communicate and interact with each other in a structured manner (article 11). Each workflow consists of predefined (and pre-translated) questions and answers.[1510] Each of the question sets is based on a specific piece of legislation supported by IMI.[1511] The question sets, like the other functionalities of IMI, have been developed by the Commission in partnership with the Member States.[1512] The Commission also has the authority to adopt implementing acts setting out the essential technical functionality and the procedural arrangements required to enable the operation of the relevant administrative cooperation procedure.[1513]

735. OTHER IMI ACTORS – Competent authorities requesting information should only provide personal data that is necessary to enable the responding competent authority to respond to the request.[1514] Likewise, competent authorities answering requests are obliged not to provide information that is irrelevant or excessive considering the identified objective of the exchange.[1515] All IMI users should carefully select which questions they include in a request and not ask for more information than is absolutely necessary.[1516] Requests for sensitive data may only be made where the processing of such data is provided for in a Union act and it is absolutely necessary to allow a decision in the particular case which is directly linked to the request.[1517]

736. ASSESSMENT – While IMI supports "free text" information exchanges[1518], the use of pre-defined workflows can help ensure that exchanged information is "adequate, relevant and not excessive" in relation to the purposes for which it is being processed. Even though the Commission is generally not involved in the administrative cooperation

---

[1510] European Commission, The Internal Market Information (IMI) System User Handbook, Update 2012, Publications Office of the European Union, Luxembourg, 2012, p. 8, available at http://ec.europa.eu/internal_market/imi-net/_docs/library/user_handbook_en.pdf.

[1511] *Id.*

[1512] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better governance of the Single Market through greater administrative cooperation: A strategy for expanding and developing the Internal Market Information System ('IMI')", 21 February 2011, COM(2011) 75 final, p. 3, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0075&rid=2

[1513] Article 11 of Regulation 1024/2012.

[1514] European Commission, Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *O.J.* 16 January 2008, p. 20.

[1515] Article 29 Data Protection Working Party, "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", *l.c.*, p. 11

[1516] European Commission, Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *l.c.*, p. 20.

[1517] *Ibid*, p. 21. See also article 16 Regulation 1024/2012. The EC Recommendation goes on to specify that IMI should not be used to conduct systemic criminal background checks (p. 21). See also European Commission, "Data protection guidelines for IMI users", *l.c.*, p. 2.

[1518] European Commission, The Internal Market Information (IMI) System User Handbook, *l.c.*, p. 21.

procedures themselves, it defines - in close collaboration with the Member States - which types of information (questions and answers) are relevant to a particular workflow. The Commission thus plays an important role in ensuring that information exchanges (a) have an appropriate legal basis (legitimacy) and (b) are limited to that which is necessary to complete a request (proportionality). The principle of finality is supported by the fact that access rights of individual IMI users shall be limited to the policy areas in which they are active.[1519] Regulation 1024/2012 does not specify how the accuracy of data exchanged through IMI shall be ensured.[1520] It does, however, specify that all IMI actors are obliged to ensure that data subjects can exercise their right to have inaccurate data corrected.[1521]

iii. Retention of data

737. BASIC PRINCIPLE – Article 14 provides that personal data processed in IMI shall be "blocked" in IMI as soon as they are no longer necessary for the purposes of administrative cooperation.[1522] Once personal data have been blocked, they may in principle only be processed for the purpose of providing proof of an information exchange through IMI.[1523] Blocked data is automatically deleted in IMI three years after the formal closure of the administrative cooperation procedure.[1524]

738. EUROPEAN COMMISSION – The European Commission is responsible for ensuring, by technical means, that personal data are in fact "blocked" once they are no longer necessary for purposes of administrative cooperation between the Member States. It must also ensure their subsequent deletion.[1525]

739. OTHER IMI ACTORS – IMI actors are encouraged to formally close administrative cooperation procedures as soon as possible after the exchange of information has been completed. Technical means are put place to enable IMI actors to involve the responsible

---

[1519] See article 9(4)-9(6) of Regulation 1024/2012. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", *l.c.*, paragraphs 37.

[1520] This is most likely due to the fact that the respective databases are governed also by national data protection regulations, which already require this information to be accurate. The primary responsibility to ensure data accuracy thus rests with the participating competent authorities.

[1521] Cf. *infra*; 744 et seq.

[1522] The precise timeframe within which personal data is "blocked" is determined in light of the specificities of each type of administrative co-operation. As a general rule, however, personal data should be blocked within six months after the formal closure of an administrative cooperation procedure. However, if a longer period is provided for in the applicable Union act, personal data processed in IMI may be retained up to 18 months after the formal closure of an administrative cooperation procedure (article 14(1) of Regulation 1024/2012).

[1523] Article 14(3) of Regulation 1024/2012.

[1524] Article 14(4) of Regulation 1024/2012. 5. At the express request of a competent authority in a specific case and with the data subject's consent, personal data may be deleted before the expiry of the applicable retention period (article 14(5)).

[1525] Article 14(6) of Regulation 1024/2012.

IMI coordinators in any procedure which has been inactive without justification for longer than two months.[1526]

740. ASSESSMENT – Given that the Commission provides and manages the software and IT infrastructure for IMI, it is only logical that it provides the technical tools necessary to enable blocking and erasure of data. The IMI Regulation goes one step further, however, by requiring the Commission to actually enforce the policy that blocked data cannot be used for purposes other than providing proof of an information exchange.[1527] It is also responsible for ensuring actual deletion of data. The obligations of the Commission are thus clearly situated at the technical level. In contrast, the responsibilities of other IMI actors seem to be of a more organisational and procedural nature. Competent authorities have a duty to formally "close" administrative cooperation procedures as soon as possible. IMI coordinators, in turn, must follow up on dormant requests to help ensure that personal data is not retained indefinitely.[1528]

iv. Transparency

741. EUROPEAN COMMISSION – Early on, the Commission began publishing on its website the sets of pre-defined questions and data fields corresponding to a particular data exchange. The EDPS immediately applauded this good practice, but also recommended that there be a legal obligation for the Commission to do so.[1529] Article 18 of Regulation 2012/2014 obliges the Commission to make publically available the "*types of administrative cooperation procedures, essential IMI functionalities and categories of data that may be processed in IMI*". It further requires the Commission to provide data subjects with information on the data protection aspects of administrative cooperation procedures, on top of its basic notice obligation under articles 11 and 12 of Regulation 45/2001.

742. OTHER IMI ACTORS – Other IMI actors are responsible for providing data subjects with information regarding their own processing of personal data through IMI, in accordance with article 10 and 11 of Directive 95/46.[1530] The Commission recommends that competent authorities, when they collect personal data directly from an individual, inform data subjects of the fact that their personal data may be processed through IMI might be disclosed to the relevant competent authorities of other Member

[1526] Article 14(7) of Regulation 1024/2012.
[1527] Article 14(6) of Regulation 1024/2012.
[1528] In this regard, the EDPS had recommended that a deadline for automatic deletion be set counting from the start of an exchange, rather than from the formal closure of a procedure. See European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01)", *l.c.*, paragraph 41. The recommendation was not adopted.
[1529] *Ibid*, paragraphs 31-32.
[1530] See also article 18(1) of Regulation 1024/2012.

States.[1531] It also recommends to provide a link to information on data protection available on the Commission's IMI website when doing so. The Commission also notes, however, that national laws exempt certain types of public authorities or procedures from the requirement to provide information.[1532] The Commission has committed itself to liaise with national IMI coordinators in order to identify the relevant national rules and to make them publicly available.[1533]

743. ASSESSMENT – Article 18 of Regulation 1024/2012 makes clear that the duty to ensure transparency of processing towards data subjects is a joint responsibility of all IMI actors.[1534] The Commission, as "operator" of the system, is best positioned to take a proactive role in providing a "first layer" of information to data subjects on its website.[1535] The active publication of information on the Commission's website allows data subjects to obtain a general overview of the functionalities and legal basis of IMI. It also provides them with an indication of where to turn in case they require more information or wish to exercise their rights as data subjects (see below). Nevertheless, the competent authorities retain their own independent obligation to adequately inform data subjects. As a rule, the competent authority shall be obliged to inform data subjects directly, unless a valid exemption applies.[1536]

v. Data subject rights

744. BASIC PRINCIPLE – In order to reduce the burden on data subjects (who are unlikely to be familiar with the technicalities of the controller relationships within IMI), Recommendation 2009/329 provided that

> "*no competent authority should refuse access, rectification or deletion on the ground that it did not introduce the data in the system or that the data subject should contact another competent authority.*"[1537]

In other words, the Commission advanced a "no wrong door" policy, to be administered primarily by the Member States. The Commission confirms this approach in its privacy statement on the IMI website.[1538]

[1531] European Commission, "Data protection guidelines for IMI users", *l.c.*, p. 2-3.
[1532] *Id.*
[1533] *Id.*
[1534] *Id.*
[1535] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", 22 November 2011, paragraph 69.
[1536] See also Article 29 Data Protection Working Party, "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", l*.c.*, p. 16 and Judgement in *Smaranda Bara and Others*, C‑201/14, EU:C:2015:638.
[1537] European Commission, European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), *l.c.*, in particular pp. 25-26.
[1538] "*If you think that your personal data is in IMI and you would like to have access to it or have it deleted or rectified, you may do so by contacting the administration or the professional body with which you had contacts or any other IMI user that was involved in the administrative cooperation procedure*

745. EUROPEAN COMMISION – The role of the Commission in actually accommodating data subject rights is limited.[1539] It provides technical support (esp. in cases where the information exchanges have already been "closed") and co-ordination between the competent authorities (in cases where a request for rectification or deletion is received and granted by a competent authority which did not initiate the information exchange).[1540] In 2009, the Commission indicated it is working on a feature that would allow online data rectification and support automatic notifications to those competent authorities involved[1541], but there seem to have been no further updates since.

746. OTHER IMI ACTORS – The competent authorities are obliged to respond within 30 days after the request by the data subject is received by the "responsible" IMI actor.[1542] As indicated above, competent authorities are encouraged to accommodate data subject rights, regardless of whether they initiated the administrative cooperation procedure within IMI or not. In principle, the competent authority receiving the request should examine it and grant or refuse it in accordance with the merits of the request (and the provisions of its own national data protection law).[1543] If needed, the competent authority may contact other competent authorities before taking a decision.[1544]

747. ASSESSMENT – Article 19 confirms that IMI actors are obliged to accommodate data subject rights. It does not, however, specify to whom data subject should direct their requests, nor does it impose a duty on competent authorities to cooperate with one and other in this respect.[1545] The practical approach advanced by the European Commission allows data subjects to exercise their rights with any competent authority who is actually involved in the procedure. The Commission could take its facilitative role one step further, by providing an online form to data subjects who believe that their personal data processed within IMI should be rectified or deleted.

---

concerning you. If you were not satisfied with the answer received, you may either contact another IMI user involved or lodge a complaint with your data protection authority." See also section 9 of Commission Privacy Statement (accessible at http://ec.europa.eu/internal_market/imi-net/_docs/data_protection/privacy_statement_en.pdf) and European Commission, "Data protection guidelines for IMI users", *l.c.*, p. 2-3, question 7.

[1539] At least insofar as it concerns personal data involved in an administrative cooperation procedure between Member States, to which the Commission is generally not a party.

[1540] See question 8 of http://ec.europa.eu/internal_market/imi-net/docs/data_protection/data_protection_guidelines_en.pdf

[1541] See European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), *l.c.,* p. 26.

[1542] Article 19 of Regulation 1024/2012.

[1543] European Commission, European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), *l.c.,* p. 25.

[1544] *Id.*

[1545] See in that sense also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", *l.c.*, paragraphs 71-73.

5.2 CROSS-BORDER IDENTIFICATION AND AUTHENTICATION (STORK AND EIDAS)

A. Introduction

748. eID INTEROPERABILITY – The EU perceives cross-border delivery of public services a necessary condition for a fully realized single market.[1546] As national eIDM systems matured, the concept of "eID interoperability" gained in political importance.[1547] Through a variety of initiatives, the EU has sought to promote the interoperability of national eIDM systems. The guiding principle in those initiatives has been the construction of a European cross-border eIDM framework, based on interoperability and mutual recognition of national eID resources and management systems.[1548]

749. STORK PROJECT – In order to advance the development of practical interoperability solutions, the EU funded a number of Large-Scale Pilot projects (LSPs). Each LSP focused on the development and testing of practical solutions in real-life cross-border public service environments.[1549] As far as eID interoperability is concerned, the most influential project by far was the STORK project.[1550] STORK, which stands for

---

[1546] European Parliamentary Research Service (EPRS), "eGovernment – Using technology to improve public services and democratic participation", July 2015, p. 9, available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA%282015%29565890_EN.pdf (last accessed 3 May 2016).

[1547] N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104. The increased emphasis on eID interoperability was particularly visible in the i2010 eGovernment Action Plan and the Roadmap for a pan-European eID Framework. See European Commission, *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, SEC(2006) 511, 24 April 2006, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0173&from=EN and European Commission, A Roadmap for a pan-European eIDM Framework by 2010, 2006, v1.0, available at http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf (last accessed 2 May 2014). The Roadmap included a list of measurable objectives and milestones for the construction of such framework. It later reconfigured the objectives with the launch of the Digital Agenda, which included two important key actions in the field of eID, namely (1) a proposal for a Council and Parliament Decision on mutual recognition on e-identification and e-authentication across the EU based on online "authentication services" to be offered in all Member States; and (2) a proposal for a revision of the eSignature Directive7 with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems. (N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104-105.) This eventually led to the adoption of Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (*O.J.* 28 August 2014, L 257/73.).

[1548] N.N.G. de Andrade, "'Electronic Identity for Europe': Moving from Problems to Solutions", *l.c.,* p. 104. See also J.C. Buitelaar, M. Meints and B. Van Alsenoy (eds.), "Conceptual Framework for Identity Management in eGovernment", *l.c.*, p. 61-64

[1549] European Commission, Directorate-General Informatics, "EU activities in the field of eID interoperability", December 2013, p. 2, available at http://ec.europa.eu/isa/documents/eu-activities-in-the-field-of-eid-interoperability.pdf.

[1550] See https://www.eid-stork.eu. The STORK project ended in 2011 and was succeeded by the STORK 2.0 project (https://www.eid-stork2.eu), which further builds on the results of STORK and also aims to develop interoperable solutions for the authentication of legal persons and mandates.

"Secure idenTity acrOss boRders linKed", set out to establish an interoperable system for EU-wide recognition of eIDs that would allow businesses, citizens and government employees to use their national eIDs in any Member State.[1551] The project produced a set of technical specifications for the interoperability of eIDs, which proved to be highly influential for the subsequent regulation of electronic identity authentication services at EU level.

750. REGULATION 910/2014 – On 4 June 2012, the European Commission published a proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market.[1552] The main objective of the proposal was to ensure the mutual recognition of electronic identification and authentication across the EU and to enhance the existing legal framework on electronic signatures.[1553] In February 2014, a political agreement was reached between representatives of the European Parliament (MEP), the Commission and the Council.[1554] The final text of the Regulation on electronic identification and trust services for electronic transactions (commonly referred to as "the eIDAS regulation") was published in the Official Journal on 28 August 2014.[1555]

751. MUTUAL RECOGNITION – Chapter II of the eIDAS regulation governs the mutual recognition of electronic identification schemes among Member States. Provided certain requirements are met, a Member State can notify its national eID scheme to the European Commission. Once an eID scheme has been notified, other Member States shall in principle be obliged to accept the electronic identification means issued under that scheme if they require electronic identification and authentication to access an online service.[1556] Of course, a Member State is only obliged to accept electronic identification

---

[1551] Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, Written Report concerning the STORK Project, Ref.Ares (2011) 424406, 15 April 2011, p. 2, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_15_letter_artwp_atos_origin_annex_en.pdf.

[1552] European Commission, Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238/2, 4 June 2012.

[1553] For more information see J. Dumortier and N. Vandezande, "Trust in the proposed EU regulation on trust services?", *Computer Law and Security Review* 2012, Vol. 28, p. 568-576 and C. Cuijpers and J. Schroers, "eIDAS as guideline for the development of a pan European eID framework in FutureID", *Open Identity Summit* 2014 vol. 237, p.23-38, accessible at https://lirias.kuleuven.be/bitstream/123456789/470230/2/OID+2014+paper+Jessica+Colette+v_final1.pdf

[1554] European Commission, "Commission welcomes political agreement on new EU regulation for electronic ID and trust services", 28 February 2014, MEMO/14/151, available at http://europa.eu/rapid/press-release_MEMO-14-151_en.htm. See also J. Schroers and B. Van Alsenoy, "Making Online Transactions Reliable and Interoperable for Europe", *LSE Media Policy Blog*, 28 May 2015, accessible at http://blogs.lse.ac.uk/mediapolicyproject/2014/05/28/making-online-transations-reliable-and-interoperable-for-europe/ (last accessed 29 November 2015).

[1555] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *O.J.* 28 August 2014, L 257/73-114.

[1556] See article 6(1)a of Regulation 910/2014. The European Commission will publish a list of notified eID schemes in the Official Journal one year from the date of application of the implementing acts referred to

means which provide an assurance level which is equal to or higher than the assurance level required by the relevant public sector body to access that service online.[1557]

752. PRACTICAL IMPLEMENTATION – The eIDAS regulation provided a legal framework for streamlining the mutual recognition of national eID schemes. Specific technical requirements for security and interoperability were left to be specified by way of implementing acts.[1558] On 9 September 2015, the European Commission published two implementing acts relevant to eID recognition, namely the implementing act on the interoperability framework[1559] and the implementing act on levels of assurance[1560].[1561] Since then, the Commission and the Member States have produced additional documentation regarding the technical interoperability architecture supporting cross-border use of eID under the Connecting Europe Facility (CEF).[1562] The technical interoperability architecture relied heavily upon the STORK architecture.[1563]

---

in Articles 8(3) and 12(8). Notifications received after that date shall be published as amendments to that list within 2 months from the date of receipt of that notification (article 9).

[1557] Article 6(1)b of Regulation 910/2014. Currently, recognition is only mandatory in cases where the relevant public sector body uses the assurance level "substantial" or "high" in relation to accessing that service online. Recognition of notified electronic identification means which correspond to the assurance level "low" is optional (article 6(2)).

[1558] See also J. Bender, "eIDAS regulation: eID – Opportunities and Risks", *25th SmartCard Workshop*, 4-5 February 2015, p. 157 available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf?__blob=publicationFile

[1559] European Commission, Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal 9 September 2015, L 235/1–6.

[1560] European Commission, Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Official Journal 9 September 2015, L 235/7-20.

[1561] See also A. Servida, The first big step in eIDAS implementation accomplished, *Digital Agenda for Europe* (blog),9 September 2015, accessible at https://ec.europa.eu/digital-agenda/en/blog/first-big-step-eidas-implementation-accomplished (last accessed 29 November 2015).

[1562] See European Commission, eIDAS – Interoperability Architecture, Version 1.00, 6 November 2015, accessible at https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf (last accessed 29 November 2015). For more information regarding the Connecting Europe Facility and its role in the implementation of Regulation 910/2014 see European Commission, Introduction to the Connecting Europe Facility eID building block, Version 1.01, accessible at https://joinup.ec.europa.eu/sites/default/files/introduction_to_the_connecting_europe_facility_eid_building_block_v1_01_0.pdf (last accessed 29 November 2015).

[1563] See also Recital (6) of Commission Implementing Regulation 2015/1501: "*Large-scale pilot STORK, including specifications developed by it, and the principles and concepts of the European Interoperability Framework for European Public Services have been taken into the utmost account when establishing the arrangements of the interoperability framework set out in this Regulation.*"

B. Functionality

753. INTEROPERABLE IDENTITY ASSURANCE – When a citizen from one Member State (the "sending Member State") wishes to access an online service offered by a public sector body in another Member State (the "receiving Member State"), the latter may require assurance of the person's identity. Obtaining such assurance requires interoperability among national identity management systems. The Commission's implementing act on the interoperability framework provides for a "network of nodes" to deliver interoperable identity assurance.[1564]

754. A NETWORK OF "NODES" – Interoperability between different eID schemes is achieved by defining the technical interfaces between so-called "nodes".[1565] A "node" is defined as

> "*a connection point which is part of the electronic identification interoperability architecture and is involved in cross-border authentication of persons and which has the capability to recognise and process or forward transmissions to other nodes by enabling the national electronic identification infrastructure of one Member State to interface with national electronic identification infrastructures of other Member States*".[1566]

A "node operator" is the entity responsible for ensuring that the node performs correctly and reliably its functions as a connection point.[1567]

755. INTEGRATION SCENARIOS – A Member State notifying a national eID scheme can choose between two integration scenarios: a "proxy-based" model or a "middleware-based" model[1568]:

(1) *Proxy-based*: the sending Member State appoints a proxy (referred to as a "C-PEPS" in the STORK project[1569]) that relays authentication information between the receiving Member State and the eID scheme of the sending Member State;

(2) *Middleware-based*: the sending Member State does not appoint a proxy but instead provides a software component ("middleware") which can be operated in the receiving Member State.

[1564] See also L. Reynolds, "The EU approach to identity assurance: an update", GOV.UK Verify (Blog), 20 November 2015, accessible at https://identityassurance.blog.gov.uk/2015/11/20/the-eu-approach-to-identity-assurance-an-update (last accessed 3 May 2016).
[1565] European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 4.
[1566] Article 2(1) of Commission Implementing Regulation 2015/1501. There are two types of nodes: eIDAS-Connectors and eIDAS-Services, collectively referred to as "eIDAS-Nodes": European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 4.
[1567] Article 2(1) of Commission Implementing Regulation 2015/1501.
[1568] European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 4. See also J. Bender, "eIDAS regulation: eID – Opportunities and Risks", *l.c.*, p. 159.
[1569] Cf. *infra*; nr. 758.

For its part, the receiving Member State can also choose between two integration scenarios: a centralized model or a decentralized model.[1570]

C. Actors

756. OUTLINE – Based on the integration scenarios mentioned above, there may be more or less actors involved in the cross-border identification and authentication of citizens. For purposes of clarity, the further analysis shall be limited to two conceptual models: the "PEPS model" and the "middleware model".

757. MIDDLEWARE MODEL – In the middleware model, the citizen authenticates himself at the relying party in the receiving Member State.[1571] The relying party uses a software component ("SPware") to handle foreign eID tokens. The user experience of the citizen is similar as if he were to access a relying party in his home country, as the components to recognize and verify her eID are integrated by SP.[1572] In this scenario, there are no intermediaries between the citizen and the relying party.[1573]

758. PEPS MODEL – In the PEPS model, the exchange of identification authentication information across Member States takes place through proxies, referred to as "PEPS".[1574] In the figure below, the C-PEPS act as the gateway to the eID system of Member State A, whereas the S-PEPS acts as a gateway for service providers in Member State B.

[1570] European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 4. See also J. Bender, "eIDAS regulation: eID – Opportunities and Risks", *l.c.*, p. 159-160.

[1571] H. Leitold, "Challenges of eID Interoperability: The STORK Project", *l.c.*, p. 146. See also H. Leitold and B. Zwattendorfer, ""STORK: Architecture, Implementation and Pilots", in N. Pohlmann a.o. (eds.), *ISSE 2010 Securing Electronic Business Processes*, Springer, 2010, p. 136-137.

[1572] *Id.* Under the eIDAS interoperability architecture, it is envisaged that middleware provided by the sending Member State may also be operated by an external operator (centralized model). See European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 4.

[1573] *Id.*

[1574] PEPS stands for "Pan-European Proxy Service". A distinction is made between two types of PEPS: C-PEPS and S-PEPS. The term "C-PEPS" (or "Citizen PEPS") refers to a proxy service located in the country of the citizen (i.e., the "sending" Member State). The term S-PEPS refers to a proxy service located in the country of the service provider (relying party) (i.e., the "receiving" Member State"). See H. Leitold, "Challenges of eID Interoperability: The STORK Project", in S. Fischer-Hübner a.o. (eds.), *Privacy and Identity Management for Life*, Springer, 2011, p. 147. In the eIDAS interoperability architecture, PEPS are collectively referred to as "eIDAS nodes". The C-PEPS reappears as the "eIDAS-service" node, whereas the S-PEPS has been rebranded as the "eIDAS-connector" node. See European Commission, eIDAS – Interoperability Architecture, Version 1.00, *l.c.*, p. 3-4.

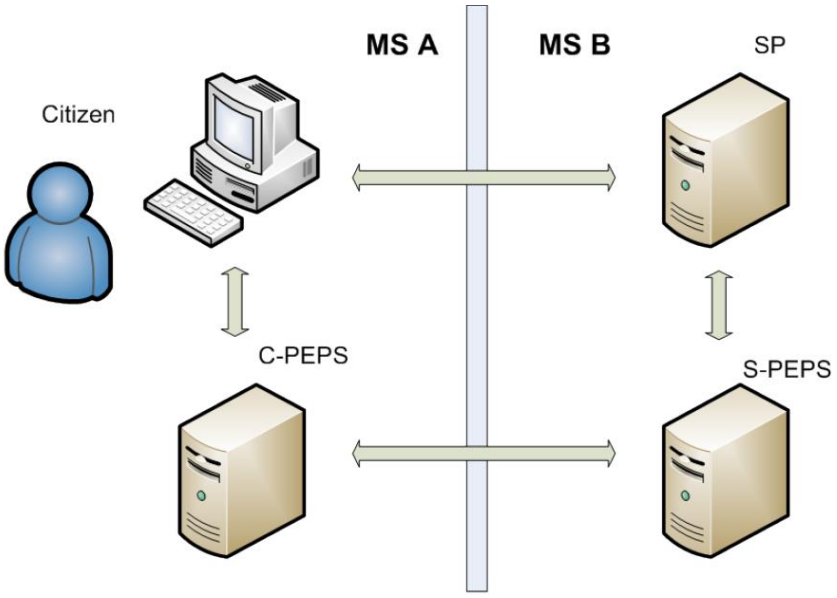

Figure 3 – The STORK "PEPS model"[1575]
© H. Leitold and B. Zwattendorfer

When a citizen of Member State A requests access to an online service in Member State B, the service provider requests assistance from the S-PEPS. The S-PEPS communicates an authentication request to the C-PEPS. The C-PEPS then triggers the identification and authentication of the citizen at the credential service provider in Member State A.[1576] Once the citizen has identified and authenticated himself towards the credential service provider, the C-PEPS transmits the relevant identity and authentication information to the S-PEPS, who can then confirm the identity of the citizen towards the service provider.[1577]

The main difference between the Middleware model and the PEPS model is that under the PEPS model the service provider delegates the handling of the identification and authentication process to a PEPS provider, whereas in the MW model the service provider takes care of this himself.[1578]

D. Roles

759. WP29 SUBGROUP – In April 2011, the Biometrics & eGovernment Subgroup of the Article 29 Working Party produced a written report concerning the STORK

[1575] H. Leitold and B. Zwattendorfer, ""STORK: Architecture, Implementation and Pilots", *l.c.*, p. 136.
[1576] Based on H. Leitold and B. Zwattendorfer, ""STORK: Architecture, Implementation and Pilots", *l.c.*, p. 136. The credential service provider (referred to as the "identity provider" in the STORK project) is not depicted in this figure.
[1577] Based on Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, Written Report concerning the STORK Project, Ref.Ares (2011) 424406, 15 April 2011, p. 4.
[1578] Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, Written Report concerning the STORK Project, Ref.Ares (2011) 424406, 15 April 2011, p. 6.

project.[1579] After describing the basic features of the Middleware and PEPS model, the Subgroup proceeded to analyse the role of the different actors involved. Interestingly, the Subgroup was unable to reach a common position regarding the legal status of the PEPS provider.

760. MIDDLEWARE MODEL – In the middleware model, the legal situation appears to be clear. Because all processing operations, including those related cross-border authentication, are performed by the service provider, the service provider is deemed responsible as the controller "*for all personal data used during the identification and authentification procedures developed and provided by STORK*".[1580]

761. PEPS MODEL – In the PEPS model, however, the legal situation was considered less straight-forward. One the one hand, it could be argued that the PEPS should be deemed a controller as far as its management of electronic identity information is concerned:

> "*He processes personal data, transfers them to another PEPS and also handles the replies (signed IDs or rejection). Although the PEPS is a service provided to different institutions (service providers "SP" in the figures above), these are not in control of what happens in the PEPS. The only thing a SP provider is in control of is to either accept or refuse the offer of a PEPS provider.*"[1581]

On the other hand, it could also be argued that the PEPS is only a processor, acting on behalf of the service providers it serves.[1582] According to the Subgroup, this interpretation had the disadvantage of increasing the number of controllers involved, thereby increasing administrative burdens.[1583] In the end, the Subgroup was not able to come to a common position: "*[s]ome of the subgroup members would consider the PEPS as controller and some as processor*."[1584]

762. APPROACH BY STORK 2.0 – In STORK 2.0, the follow-up project to STORK, the following position was adopted in relation to the PEPS operators:

> "*The PEPS operator acts as a data processor to the SP for the authentication processes conducted on behalf of the SP, with the SP acting as the data controller. This is reasonable, because this processing of personal data is done at the request of the SP, who can thus be said to control the means (it has chosen to use the PEPS) and the purposes (it has a need to authenticate the end user) of the processing. The PEPS operator on the other hand has no own purposes in this processing, and has not chosen the means to be used in the authentication process.*

[1579] Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, Written Report concerning the STORK Project, Ref.Ares (2011) 424406, 15 April 2011.
[1580] *Ibid*, p. 6.
[1581] *Id*.
[1582] *Ibid*, p. 6-7.
[1583] *Ibid*, p. 7
[1584] *Id*.

The PEPS operator acts as a data controller for any other processing of personal data, notably any logging of authentication processes that may be done by the PEPS. These are not done for purposes determined by the SP, but rather for public interest purposes (to support accountability). No processors are used for these types of processing of personal data."[1585]

763. ASSESSMENT – The approach advanced by the STORK 2.0 project differentiates between processing operations in light of the *interests served* by the processing activity. The service provider has a direct interest in the outcome of an authentication process. He is therefore considered to be the controller in relation to the processing of personal data as part of the authentication process. As far as these operations are concerned, the PEPS operator is considered a mere processor. The PEPS operator is viewed as a controller, however, in relation to "other" processing activity, such as logging. The distinction may seem somewhat artificial, as logging is an integral part of the authentication process designed to help ensure its security. The argument could therefore easily be made that a service provider should also be considered a controller in relation to log entries that correspond with its authentication requests.

E. Responsibilities

764. A WORK IN PROGRESS – In contrast with the IMI Regulation (cf. *supra*), the eIDAS regulation does not specify how the actors involved should cooperate in order to comply with data protection law. Article 11 of the eIDAS regulation governs the liability of the "party issuing the electronic identification means" and the "party operating the authentication procedure", but only insofar as its obligations under the eIDAS regulation itself are concerned.

765. WP29 RECOMMENDATIONS – In its written report concerning the STORK project, the subgroup of the Article 29 Working Party recommended the development of (1) common minimum standards for data security; (2) harmonised retention period for log files; (3) procedures to ensure transparency towards data subjects; and (4) specific recommendation on how the principles of data minimisation should be implemented and taken into consideration by service providers.[1586]

[1585] H. Graux, "Consolidated Data Protection Report", *STORK 2.0*, Deliverable D3.8, 9 October 2015, p. 22-23, available at https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=74:d38-consolidated-data-protection-report&Itemid=175 (last accessed 30 November 2015).

[1586] See also H. Graux, "Initial Data Protection Report", *STORK 2.0*, Deliverable D3.7, 20 November 2012, available at https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=9:d37-initial-data-protection-report&Itemid=175 (last accessed 30 November 2015).

766. MEMORANDUM OF UNDERSTANDING – Following the correspondence with the Article 29 Working Party, the STORK 2.0 project developed a Memorandum of Understanding (MoU) which covers certain data protection aspects, namely:

(1) Legitimacy: processing of personal data by PEPS shall require the prior informed consent of the individual concerned following a common approach;

(2) Transparency: a model privacy policy and substandard practice for providing notice to individuals;

(3) Confidentiality and security: PEPS are expected to implement STORK's security guidelines.[1587]

767. OPINION OF THE EDPS – In his Opinion on the draft proposal of the eIDAS regulation, the EDPS recommended a harmonized European approach to data protection issues surrounding crossborder identification and authentication.[1588] In particular, the EDPS emphasized the need to address (1) data security[1589]; (2) transparency and individual control[1590]; (3) the categories of data involved in the identification and authentication of individuals[1591]; (4) use of privacy-enhancing technologies[1592]; (5) requirements for the issuers of national eID schemes.[1593] While certain aspects of the EDPS recommendations were integrated in the final version of the eIDAS regulation, it is clear that a comprehensive and harmonised approach is yet to emerge.

6 EVALUATION

768. A COMPLEX ENVIRONMENT – eGovernment identity management systems involve a wide range of actors. The preceding sections have illustrated that it can be difficult, even for experts, to determine the precise role of each actor involved. There are at least two factors which complicate the analysis. First, there is the *distribution of influence* over the processing. In eGovernment identity management, different actors influence the processing at different stages and to different degrees. Only rarely does a single actor exercise complete and exclusive control over a given processing activity. Second, eGovernment identity management involves a wide range of *supporting services*

[1587] H. Graux, "Consolidated Data Protection Report", *l.c.*, p. 25-30.
[1588] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation), 27 September 2012, at paragraph 14 https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-27_Electronic_Trust_Services_EN.pdf
[1589] *Ibid*, paragraph 19.
[1590] *Ibid*, paragraph 21.
[1591] *Ibid*, paragraph 27.
[1592] *Ibid*, paragraphs 23 and 28.
[1593] Ibid, paragraph 32.

(e.g., verification, integration) which are operated independently of the specific information exchanges they facilitate.

769. HYBRID ROLE OF INTERMEDIARIES – Intermediaries, such as IMI or PEPS, promote interoperability among public administrations. While the services they provide mainly benefit the interests of their end-users (the intermediary in principle has no direct interest in the information being exchanged), the end-users have only limited influence over the design and operation of these services. This finding does not, by itself, disqualify end-users from being controllers. It does beg the question, however, whether such intermediaries should be considered as mere processors. After all, these entities exercise a determinative influence on how the processing shall be organised in order to achieve a particular purpose. The two case studies presented in this chapter illustrate the difficulties surrounding the hybrid role of intermediaries.

770. INTERNAL MARKET INFORMATION SYSTEM – In the case of IMI, the European Commission was labelled a controller for its role in the design and operation of the IMI system.[1594] Its legal relationship with other IMI actors, however, remains blurry. Initially the Commission was labelled a joint controller, more recently it was implied that the Commission acts a separate controller. The controllership status attributed to the Commission for its role in IMI appears similar to the status given by the Article 29 Working Party to the operators of so-called "e-Government portals".

771. E-GOVERNMENT PORTALS – In Opinion 1/2010, the Article 29 Working Party made the following observations regarding the role of e-Government portals:

> "*E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit.*"[1595]

772. CRITIQUE – Lokke Moerel has extensively criticized the interpretation put forth by the Article 29 Working Party in relation to e-Government portals.[1596] Specifically, she

---

[1594] The Commission is not always clearly identified as a "controller". The Commission has more frequently been referred to as the "operator" of the system. Regulation 1024/2012 does not explicitly state whether the Commission is a controller or not.

[1595] Opinion 1/2010, *l.c.*, p. 21.

[1596] L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, Oxford, Oxford University Press, 2012, p. 221-223.

argues that the Working Party mistakenly attributes controllership based on the portal's ability to decide about certain *aspects* of the processing (e.g., security), without also deciding about the purposes and means of the underlying processing operations.[1597] Moerel views the Working Party's construction as a *strategic* interpretation, designed to render the portal provider directly accountable for certain aspects of the processing, which under the current framework is only possible by attributing controllership:

> "*The fact that the third-party provider probably decides also on the security measures for the portal (and is probably best positioned to do so), does not change the fact that he does not have decision-making power as to the purposes and means of the processing. Though I agree with the Working Party 29 that it may be advisable to make data processors (in addition to controllers) responsible for data security, this should be achieved by making (also) the data processor directly responsible for the security of processing in the revised Directive, rather than through a creative interpretation of the concept of controller*."[1598]

773. ASSESSMENT – In my view, it is not surprising that the Article 29 Working Party considers the operators of e-Government portals as controllers. It is possible to distinguish, at least in theory, between *control over a system* and *control over specific processing activities within that system*.[1599] In practice, however, it is not always easy to establish when an intermediary "controls a system" or merely "operates a system on behalf of others".[1600] Moreover, it is not always clear what the implications are in terms of the distribution of responsibility and risk. If intermediaries and end-users fail to agree on appropriate measures, who carries the risk? Does system responsibility imply co-control (leading to joint liability) or is it separate control (leading to separate liability)? Are they obliged to put in place a legally binding arrangement that ensures compliance with data protection requirements?

774. PAN-EUROPEAN PROXY SERVICE – The example of the Pan-European Proxy Service (PEPS) further illustrates the practical difficulties that may arise when applying the existing concepts to e-Government intermediaries. Despite the additional guidance contained in Opinion 1/2010, the Biometrics & eGovernment Subgroup was unable to come to a common position as to whether the operator of a PEPS should be deemed a controller or a processor. The reasoning of the Subgroup suggests that the final outcome may be more a result of framing rather than the straight-forward application of established criteria. If one emphasises the autonomous design of the service, or the limited choices available to end-users, one winds up concluding that the PEPS operator acts as a controller. Conversely, if one emphasizes the auxiliary nature of the service,

---

[1597] L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 221.
[1598] *Ibid*, p. 222
[1599] See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, 59 and M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 374.
[1600] See also *infra*; nr. 1112 et seq.

designed to serve the interests of others, one winds up concluding that the PEPS operator should be deemed a processor.

775. IMI: A PRAGMATIC APPROACH – Regulation 1024/2012 provides a relatively comprehensive data protection framework for IMI.[1601] After 5 years of incremental progress, the main responsibilities of each actor have been set forth in a binding legal instrument. The final distribution of tasks seems driven more by pragmatic than by formal considerations. The Commission, as co-ordinator and operator of the IMI system, is best placed to assume responsibility for data protection requirements that concern the system as such (e.g., security, transparency regarding the functionalities of IMI). The competent authorities, on the other hand, must remain obliged to use the system responsibly and collaborate in the accommodation of data subject rights. Questions of who is controller, joint controller or processor seem to have had a limited impact. Any lingering conceptual ambiguity was overcome by simply focusing on how responsibilities should be allocated.

776. INCENTIVES AND GUIDANCE – The IMI system was scrutinized once by the Article 29 Working Party, and twice by the EDPS. As a Pan-European eGovernment initiative, IMI was subject to more scrutiny than most information exchange systems. In the private sector, similar scrutiny is typically lacking. While each end-user of an information exchange system shall in principle be considered a controller, the legal status of operator of the system may be less clear. As such, the operator may be less inclined to co-ordinate the implementation of practical measure to comply with data protection requirements.[1602] Additional incentives and guidance may be needed to ensure that system operators develop and operate their systems in a manner which facilitates compliance by end-users.

[1601] Certain issues are yet to be addressed, however, such as the use of national unique identifiers.
[1602] In fact, the operator may even be incentivized to abstain from such co-ordination as much as possible: the more he influences the "essential elements of the processing", the less likely he shall be considered a mere processor.

Chapter 3 ONLINE SOCIAL NETWORKS

1 INTRODUCTION

777. THE RISE OF OSNs – One of the most significant developments in the online environment over the past decade has been the rise of social media.[1603] More and more individuals are making use of online social networks (OSNs) to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. But users are not the only ones who are interested in OSNs. OSNs have come to attract a wide range of actors, which include application developers, web trackers, third-party websites, data brokers and other observers.

778. OUTLINE – The objective of this chapter is to analyse how the current data protection framework relates to the context of OSNs. To this end, it will begin by describing the various actors engaging with OSNs and the interactions between them. Next, it will analyse the legal status ("role") of each actor, as interpreted by regulators, scholars and courts. After that, it will describe the main responsibilities assigned to each actor, in particular by the Article 29 Working Party and national regulatory authorities. Once this analysis has been completed, this chapter will critically evaluate the relationship between the current framing of roles and responsibilities and the context of online social networking.

2 ACTORS

779. SELECTION CRITERIA – The current inventory of actors is based on a literature study of academic publications, regulatory guidance and news articles concerning privacy and data protection in OSNs. A common denominator among the selected entities is that they each process personal data resulting from (a) the usage of OSNs and/or (b) the usage of other services which somehow interact with the OSN.

780. ACTORS OVERVIEW – The following eight actors may be considered as being particularly relevant to online social networks from a data protection and privacy perspective:

(1) OSN users;

(2) OSN providers;

(3) (Third-party) application providers;

(4) (Third-party) trackers;

[1603] O. Tene, "Privacy: The new generations", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 22.

(5) (Third-party) data brokers;

(6) (Third-party) website operators;

(7) Other observers; and

(8) Infrastructure service providers.

781. VISUAL REPRESENTATION – The aforementioned actors interact with each other in a variety of ways. The following figure provides a -highly simplified- representation of how these actors typically interact with OSNs and OSN-related data. It is intended to be conceptual rather than factual.

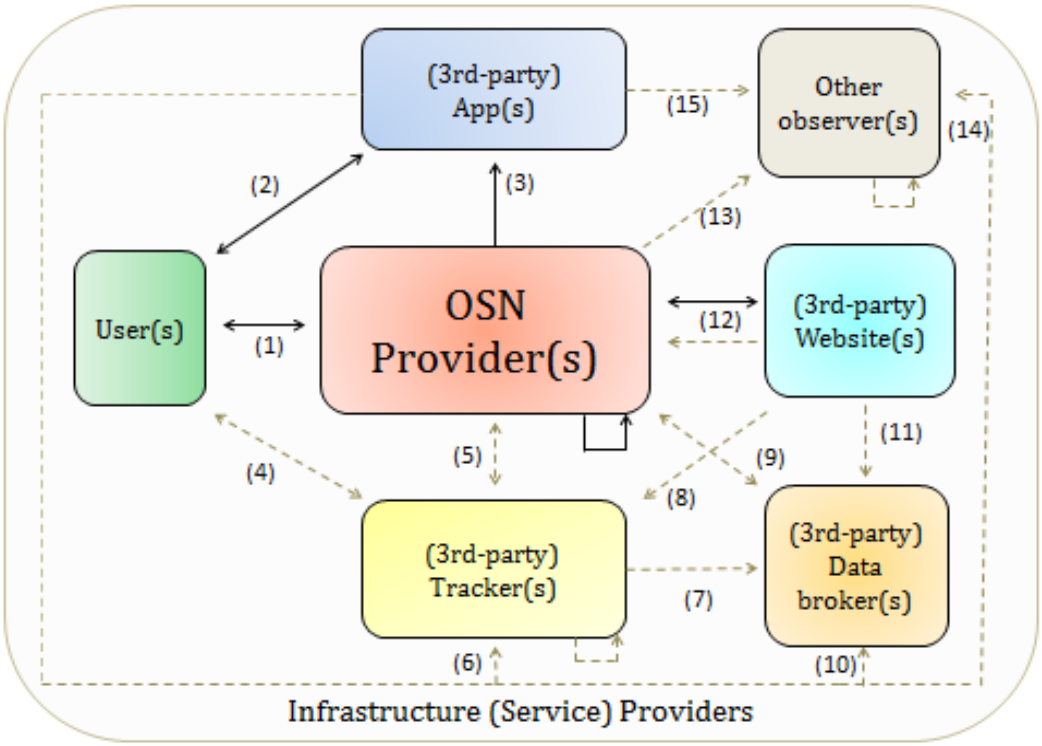

Figure 4 – Main OSN actors

782. LEGEND – The arrows in Figure 4 indicate that an exchange of personal data is taking place. This exchange can be either uni- or bi-directional. Solid black arrows signify exchanges of personal data which occur primarily "in the foreground", meaning that they can easily be observed or inferred by OSN users. They typically imply some form of active involvement by OSN users (e.g., granting a permission, manually entering data, use of an application). Dashed grey arrows were used to signify data exchanges which are likely to be less obvious to OSN Users. Some of these exchanges may be detectable (e.g., by monitoring the activities of one's internet browser) or otherwise ascertainable (e.g., by reading the privacy notice of an OSN provider).[1604] Others may

[1604] Even if users are notified of their existence at a certain point in time, they may not be consciously aware of them at a later stage, as these exchanges typically occur "in the background" or do not require active user involvement.

occur completely unnoticed. Over the following sections, a brief description is provided of each of the actors and interactions displayed in Figure 4.

783. COMBINATIONS POSSIBLE – The reader should note that the categories of actors identified in Figure 4 are not mutually exclusive. A given actor may combine multiple roles depending on the circumstances (e.g., an OSN provider might also deploy its own tracking mechanisms, or an application provider might also be the operator of a third-party website).

2.1 OSN USER

784. MAIN CHARACTERISTICS – An OSN user is, as the name suggests, any individual who makes use of an OSN. People can join OSNs in different capacities. Individuals acting in a personal capacity typically join an OSN to stay in touch with friends and family, to connect around shared interests or hobbies, or to make new friends.[1605] Increasingly, however, OSNs are also used by companies and other organisations to advance commercial, political or humanitarian goals.[1606]

785. DATA DISCLOSURE – Individuals can disclose a great deal of information about themselves when making use of OSNs. The creation of an OSN account (or "profile") involves disclosure of a number of attributes, which typically include name, date of birth and place of residence. Most OSNs also encourage its users to upload a picture of themselves.[1607] Depending on the nature of the OSN, users might be encouraged to reveal additional information such as relationship status and interests (e.g., Facebook) or current employment (e.g., LinkedIn). Once a user has signed up, he or she is essentially free to share any information they see fit. This information can range from mundane facts (e.g., "I'm at the mall"), to political views (e.g., "vote 'no' on prop 11"), to highly intimate personal details (e.g., "I'm dating Alice but I think I'm in love with Bob"). Even though the policies of an OSN may impose certain restrictions, OSN users are also in a position to disclose information about others. Finally, it is worth noting that a significant amount of personal data disclosed via OSNs is relational. Social connections among OSN users can be used to create a "social graph", whereby nodes represent users

[1605] A. Smith, "Why Americans use social media", *Pew Internet & American Life project*, 15 November 2011, available at http://pewinternet.org/Reports/2011/Why-Americans-Use-Social-Media.aspx (last accessed 17 December 2013).

[1606] See e.g. J. Heidemann, M. Klier and F. Probst, "Online social networks: A survey of a global phenomenon", *Computer Networks* 2012, vol. 56, p. 3871-3872 (discussing potential usage by businesses); R.D. Waters, E. Burnett, A. Lamm and J. Lucas, "Engaging stakeholders through social networking: How nonprofit organisations are using Facebook", *Public Relations Review* 2009, Vol. 35, Issue 2, p. 102–106. See also Article 29 Working Party, "Opinion 5/2009 on online social networking", WP163, p. 7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (last accessed 17 December 2013).

[1607] d.m. boyd and N.B. Ellison, "Social Networking Sites: Definition, History and Scholarship", *Journal of Computer-Mediated Communication* 2008, vol. 13, p. 211-212.

and connections or edges represent the relationships between these users.[1608] In addition, certain OSN features expose additional relational information (e.g., group formation).

786. DATA FLOWS – At the end of the day, OSN users disclose considerable amounts of information about themselves. They also access significant amounts of information related to others. This flow of personal data is depicted in Figure 4 as bi-directional arrow (1).

2.2 OSN PROVIDER

787. MAIN CHARACTERISTICS – An OSN provider is an entity that operates the hard- and software necessary to deliver an OSN service.[1609] According to boyd and Ellison, the key features of social network sites are that they allow individuals to

> *(1) "construct a public or semi-public profile within a bounded system;*
>
> *(2) articulate a list of other users with whom they share a connection; and*
>
> *(3) view and traverse their list of connections and those made by others within the system."*[1610]

788. DATA COLLECTION – OSN providers collect various types of data about their users. Schneier has developed a taxonomy of "social networking data", which distinguishes among the following six categories of data[1611]:

1. *Service data*: data provided to an OSN provider in order to make use the OSN (e.g., legal name, age);
2. *Disclosed data*: data that is posted by OSN users on their own profile pages (e.g., blog entry, picture, video);

[1608] R. Sayaf and D. Clarke, "Access control models for online social networks", in *Social Network Engineering for Secure Web Data and Services*, IGI, 2013, p. 2.; G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), "Online Social Networks: Status and Trends", *New Directions in Web Data Management*, Studies in Computational Intelligence, Vol. 331, 2011, p. 215.

[1609] A reference architecture of OSNs can be found in G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), "Online Social Networks: Status and Trends", *l.c.*, p. 217.

[1610] d.m. boyd and N.B. Ellison, "Social Networking Sites: Definition, History and Scholarship", *l.c.*, p. 211. This definition has been criticized by Beer as being too broad: see D. Beer, "Social network(ing) sites … revisiting the story so far: A response to danah boyd & Nicole Ellison", *Journal of Computer-Mediated Communication* 2008, Vol. 13, p. 516 et seq. See also J. Heidemann, M. Klier and F. Probst, "Online social networks: A survey of a global phenomenon", *l.c.*, p. 3867. Like Heidemann, I use the term Online Social Networks to refer to "user-oriented" (as opposed to "content-oriented") social network sites; which emphasize social relationships and communities. The distinction between "content-oriented" and "user-oriented" social networks was proferred by G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), "Online Social Networks: Status and Trends", *l.c.*, 2011, p. 220.

[1611] B. Schneier, "A Taxonomy of Social Networking Data", *Security & Privacy* 2009, IEEE, Vol. 8, Issue 4, p. 88.

3. *Entrusted data*: data that is posted by OSN users on the profile pages of other OSN users (e.g., a wall post, comment);
4. *Incidental data*: data about an OSN user which has been uploaded by another OSN user (e.g., a picture);
5. *Behavioural data*: data regarding the activities of OSN users within the OSN (e.g., who they interact with and how); and
6. *Derived data*: data which is inferred from (other) OSN data (e.g., membership of group X implies attribute Y).

789. DATA USAGE – The data collected by OSN providers are used to enable various forms of social interaction. While the display of user profiles may be considered the "backbone"[1612] of an OSN, many platforms offer an array of additional features and services. OSNs typically provide common messaging services (e.g., chat, email), as well as message board and commenting functions.[1613] An OSN provider can also use the personal data of its users to support its business model. In fact, the primary source of revenue for most OSN providers is derived from advertising.[1614] These business models are based on the principle that "free" services can attract large and diverse audiences, which in turn will attract advertisers.[1615] Popular OSNs, which have a large number of active users, can develop rich sets of demographic and behavioural data.[1616] The profile information of these users, together with information about their activities (e.g., web browsing, app usage, "likes", current location, etc.), can be used to enhance audience segmentation and contextual awareness.[1617] This ability is of great interest to

[1612] d.m. boyd and N.B. Ellison, "Social Networking Sites: Definition, History and Scholarship", *l.c.,* p. 211.
[1613] J. Heidemann, M. Klier and F. Probst, "Online social networks: A survey of a global phenomenon", *l.c.*, p. 3867.
[1614] For an early analysis of different revenue models for OSN see A. Enders, H. Hungenberg, "The long tail of social networking. Revenue models of social networking sites", *European Management Journal* 2008, Vol. 26, p. 199– 211. For a more recent study see G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), "Online Social Networks: Status and Trends", *l.c.*, 2011, pp 213-234. Alternative and/or additional revenue sources include subscription fees (e.g., for "premium" accounts) and platform purchases (e.g., by charging a percentage on the purchase of apps or other products which were bought through the OSN platform).
[1615] G. Pallis, D. Zeinalipour-Yazti and M.D. Dikaiakos in A. Vakali and L.C. Jain (eds.), "Online Social Networks: Status and Trends", *l.c.*, p. 221.
[1616] *Ibid*, p. 222.
[1617] Facebook, for example, enables third parties to target advertisements to its users on the basis of location, gender, age, likes and interests, relationship status, workplace and education (see https://www.facebook.com/help/207847739273775). (See also R. Heyman and J. Pierson, "An Explorative Mapping of the Belgian Social Media Value Network and its Usage of Personal Identifiable Information", paper presented at *IFIP Summerschool on Privacy & Identity Management* 2013, p. 2.) In April of 2013, Facebook added "partner categories" as an additional targeting feature, which enables advertisers to target individuals based on the basis of their purchase behaviour outside the social network. See https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature (last accessed 17 December 2013). For a survey of different targeting methods using social networking information see A. Bagherjeiran, R.P. Bhatt, R. Parekh and V. Chaoji, "Online Advertising in Social Networks", in B. Furht (ed), *Handbook of Social Network Technologies and Applications*, 2010, Springer, New York, p. 653 et seq.

advertisers, who are eager to see advertisements presented to users who are likely to be influenced by them.

790. DATA FLOWS – The data flows which facilitate behavioural targeting are represented in Figure 4 by arrows (4) through (10). Each of these data flows will be elaborated further over the following sections.

2.3 (THIRD-PARTY) APPLICATION PROVIDER

791. MAIN CHARACTERISTICS – Third-party applications (often referred to simply as "apps") have become a popular feature on OSNs.[1618] An app is a standardised piece of software that runs on a computing platform.[1619] In principle, an app can provide just about any functionality: gaming, content streaming, location sharing, crowd funding … the possibilities are endless. Several major OSN providers now allow third-party application developers to offer their apps through the OSN.[1620]

792. DATA COLLECTION – App usage is generally predicated upon the granting of permissions. Permissions requested by application providers typically concern access rights (e.g., the ability to access to profile information, photo's, etc.) and/or the ability to act on the user's behalf (e.g., to post on a message board or send an email on behalf of the user).[1621] Once permissions have been granted, the application provider can use these privileges to collect personal data about the user from the OSN provider. It can also collect additional information from users directly (e.g., by monitoring application usage).

[1618] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *Proceedings of ACM Conference on Online Social Networks* (CSON) 2013, preprint version available at http://www.sba-research.org/wp-content/uploads/publications/AppInspect_peprint.pdf

[1619] OECD, "The App Economy", *OECD Digital Economy Papers* 2013, No. 230, OECD Publishing, available at http://dx.doi.org/10.1787/5k3ttftlv95k-en (last accessed 19 December 2013). Apps can be divided among two main categories: "mobile" or "web-based". In case of mobile apps, the "computing platform" that hosts the app is a mobile device, typically a smartphone or a tablet. In case of web-based apps, the app itself is hosted on a webserver which is controlled by the application provider. While mobile apps are stored on a smartphone rather than a webserver, many mobile apps still communicate with a webserver. For purposes of conceptual clarity, we will approach our discussion of third-party applications under the assumption that they are web-based, except when explicitly indicated otherwise. For an in-depth discussion of mobile apps on smart devices see Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", WP202, 27 February 2013, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last accessed 20 January 2014).

[1620] W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", in L. Caviglione, M. Coccoli and A. Merlo (eds.), *Social Network Engineering for Secure Web Data and Services*, IGI Global, 2013, p. 207 et seq.

[1621] In practice, the OSN user delegates one or more access rights to the application provider using a pre-determined protocol (e.g., OAuth). Once the permissions have been granted, the application provider will query the social network application programming interface (API) to make use the delegated privileges (e.g., access profile information, post to wall). (W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 208). See also M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 1-2.

793. DATA USAGE – Third-party application providers may use data about OSN users in a variety of ways. Some apps are "socially aware", meaning that they consume OSN data (e.g., profile data, relationship information) to deliver their functionality. For example, a horoscope application might require the birthdates of you and your contacts in order to create a compatibility chart. Other apps do not require user data to function as such, but use them to incorporate other aspects of social networking.[1622] For example, users might be encouraged to share gaming high scores or to display which music feeds they are listening to on their profile. As in the case of OSN providers, data collected by application providers is often also used to facilitate behavioural advertising, particularly when users are able to use an app without monetary payment.

794. DATA FLOWS – While an app may be accessible through an OSN website, the app itself typically runs on a third-party server (i.e., outside the OSN domain).[1623] In order to make app usage an integral part of the user experience, the OSN provider can embed applications within the OSN website (e.g., as an iframe).[1624] In this approach, the OSN provider effectively acts as a proxy between users and third-party application providers.[1625] Alternatively, the OSN provider can simply direct its users to the websites of the application providers. The data flows among application providers, OSN providers and OSN users are depicted in Figure 4 as arrows (2) and (3). Arrow (2) is bi-directional because application providers may also send their users data about other users (e.g., music feeds or current location).

2.4 (THIRD-PARTY) TRACKER

795. MAIN CHARACTERISTICS – In the context of this chapter, the term "tracker" is used to describe any entity that collects and/or analyses data relating to the internet browsing activities of OSN users.[1626] There are many different ways of tracking individuals online.[1627] The most well-known technique involves the use of "cookies".[1628]

[1622] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 2.

[1623] *Id.* In earlier implementation models, social applications were deployed on the infrastructure of the OSN itself (this model is sometimes referred to as the "gadget paradigm"). Increasingly, however, a different model is followed, whereby applications are delivered through an Applications Programming Interface (API) (also referred to as the "distributed" paradigm). (W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 208.)

[1624] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 2. See also W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 211 et seq.

[1625] *Ibid*, p. 1.

[1626] The term "third party" is bracketed to indicate that several OSN provider deploy their own tracking technologies to monitor user behaviour inside and outside the OSN.

[1627] See C. Casteluccia, "Behavioural Tracking on the Internet: A Technical perspective", S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, 2013, Springer Science+Business Media, p. 21 et seq. for an inventory of prevalent web tracking techniques.

[1628] A cookie is an alphanumeric text file which is stored by a web browser. Cookies are typically set by web servers the first time a user visits a particular site. They are then sent back automatically by the browser each time it accesses the web server that placed them. (C. Casteluccia, "Behavioural Tracking on

Cookies are browser files deployed by website operators in order to keep track of their interactions with a particular visitor.[1629] On many websites, individuals also receive cookies emanating from third party domains ("third-party cookies"), which can be used to monitor their browsing behaviour across different websites.[1630] Other well-known tracking techniques involve use of javascripts and browser fingerprinting.[1631]

796. DATA COLLECTION – A 2008 study by Krishnamurthy and Wills found that individuals' activities on OSN may be subject to third-party tracking. Specifically, they found that several user actions (e.g., logging in, viewing a profile page, leaving a message) on OSNs such as Facebook and Myspace resulted in the retrieval of objects from third-party domains.[1632] The access of third-party domains in this context suggested that OSN users may be tracked by third parties even when they are engaged in social networking activities (in addition to being tracked during other browsing activities).[1633] In a follow-up study, the same authors found that many OSNs also leaked additional information about OSN users, such as name, gender or OSN unique ID.[1634] This means that the browsing behaviour of a particular OSN user – including his or her behaviour outside of the OSN context – may be easily linked to his or her OSN identity.[1635]

797. DATA USAGE – By monitoring individuals' browsing activities over time, trackers are able to build rich behavioural profiles. These profiles can in turn be used for online behavioural advertising (OBA), which is an important source of revenue for trackers.[1636]

---

the Internet: A Technical perspective", *l.c.*, p. 23-24 and Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", WP 171, 22 June 2010, p. 7, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed 3 January 2013).

[1629] This technique may be particular useful for identifying returning visitors and recording user preferences (e.g. language preferences).

[1630] For example, a web page may contain images, links, iframes or other components stored servers in other domains. When the user accesses the website, these components will be retrieved from the third-party domain, which allows for the placement of third-party cookies. This technique can be used to effectively track users across multiple sites (in particular across all pages where one has placed an advertising image or web bug) (C. Casteluccia, "Behavioural Tracking on the Internet: A Technical perspective", *l.c.*, p. 23-24.)

[1631] See C. Casteluccia, "Behavioural Tracking on the Internet: A Technical perspective", *l.c.*, p. 21 et seq.

[1632] B. Krishnamurthy and C.E. Wills, "Characterizing Privacy in Online Social Networks", *WOSN* 2008, Proceedings of the 1st ACM workshop on Online social networks, 2008 p. 40.

[1633] *Ibid*, p. 41.

[1634] B. Krishnamurthy and C.E. Wills, "On the Leakage of Personally Identifiable Information Via Online Social Networks", *WOSN 2009*, Proceedings of the 2nd ACM workshop on Online social networks, 2009, p. 7. See also C. Casteluccia, "Behavioural Tracking on the Internet: A Technical perspective", *l.c.*, p. 28.

[1635] *Id.* See also J. Cheng, "Social networks make it easy for third parties to identify you", *Ars Technica*, 25 September 2009, available at http://arstechnica.com/security/2009/09/which-user-clicked-on-viagra-ads-ask-myspace-and-facebook (last accessed 7 January 2013).

[1636] The Article 29 Working Party defines behavioural advertising as advertising which is based on the observation of the behaviour of individuals over time. By studying the characteristics of individuals' behaviour over time (repeated site visits, interactions, keywords, etc), trackers can develop specific profiles on individuals, which in turn allows tailoring advertisements to the inferred interests of each individual concerned. (Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", *l.c.*, p. 4).

In many cases, third-party trackers work on behalf of ad networks, whose goal it is to target ads with the maximum effect possible.[1637]

798. DATA FLOWS – The data flows related to tracking of OSN users are depicted in Figure 4 by arrows (4) and (5). Arrow (4) represents tracking which occurs via the browsers of OSN users (arrow (4)). In this scenario, the OSN provider does not directly share information about the user with trackers. Instead, it is sufficient for the OSN provider to embed components which result in the retrieval of third-party objects.[1638] Arrow (5) depicts the data flows which take place in situations where an OSN provider actively collaborates with a tracker. This might occur, for example, in situations where the tracker is working on behalf of the OSN provider (e.g., if the OSN provider wishes to collect data about its users browsing activities outside the OSN).[1639] Many application providers and third-party websites also embed components which facilitate third-party tracking and ad delivery. This is depicted in Figure 4 by arrows (6) and (8).[1640]

2.5 (THIRD-PARTY) DATA BROKER

799. MAIN CHARACTERISTICS – Data brokers (also referred to as "data aggregators" or "information resellers") are entities which collect and sell information. To be more specific, a data broker is a company that collects data, including personal data, from a wide variety of sources with a view of turning these data into marketable commodities.[1641] Among the products offered by data brokers are consumer profiles (which categorize individuals into pre-determined consumer segments) and scoring

[1637] An ad network is an entity that connects website owners ("publishers") with advertisers. In this model, a website owner simply needs to reserve a certain amount of visual on its website that will serve to display ads and relinquish the rest of the process to one or more ad network providers. The ad network provider is then responsible for distributing advertisements to publishers (on behalf of companies seeking to advertise). (Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", *l.c.*, p. 5.) As indicated earlier, the OSN providers may offer targeting options which function independently of third-party trackers, using criteria derived from e.g. the profile information of their users. In this model, the OSN provider uses its own targeting technology and makes its own decisions about ad placement and distribution (in accordance with advertiser demands).

[1638] Arrow (4) is bi-directional arrow because every time a user accesses a webpage which links to the tracker's server, the cookie that is stored in the user's browser will be updated with data about the user's latest interactions.

[1639] The term "third party" is bracketed to indicate that several OSN provider deploy their own tracking technologies to monitor user behaviour inside and outside the OSN.

[1640] Arrows (6) and (8) are misleading to the extent that tracking occurs via the browser or operating system of the user (in which case it would simply coincide with arrow (4). The reason for choosing this form of visual representation is to make clear that users can be tracked across a wide range of activities, i.e., across web browsing, OSN usage and app usage.

[1641] Based on Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, March 2012, p. 68, available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

products (which score the likelihood for certain behaviours, based on inferences drawn from other data).[1642]

800. DATA COLLECTION – Data brokers collect data from a wide variety of sources. Several data brokers also collect data about individuals from OSN sites.[1643] For example, data broker Acxiom reportedly collects data regarding individuals' social media usage to predict whether he or she should be considered a "heavy social media user", "poster", "video sharer", "social influencer", or "social influenced".[1644]. Several data brokers reportedly also use click-stream data (i.e. data relating to individuals' browsing behaviour) in developing consumer profiles.[1645]

801. DATA USAGE – Information collected by data brokers is put to a variety of uses. Prominent examples include identity verification, fraud prevention, marketing, credit risk assessments and background checks.[1646] Some data brokers also offer products that enable marketers to use off-line data to target individuals online.[1647] These products can also be put to use in an OSN context. Facebook, for example, has partnered with data brokers such as Acxiom, Datalogix and Epsilon so that advertisers can target OSN users on the basis of their purchasing behaviour outside the social network.[1648] Facebook has reportedly also partnered with data broker BlueKai to enable further targeting of OSN users on the basis of their browsing activities outside the OSN.[1649]

[1642] U.S. Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes", Staff Report for Chairman Rockefeller, 2013, p. 12 and 23 available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 (last accessed 6 January 2014).

[1643] Other avenues include government records and other public data, purchase or license from other data collectors, cooperative agreements with other companies, self-reporting by consumers (e.g., through surveys or questionnaires). U.S. Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes", *l.c.*, p. 15.

[1644] *Ibid*, p. 21.

[1645] *Id.* See also OECD, "Exploring data-driven innovation as a new source of growth: Mapping the policy issues raised by "big data"", in OECD, Supporting Investment in Knowledge Capital, Growth and Innovation, 2013, OECD Publishing, doi: 10.1787/9789264193307-12-en, p. 328, available at http://www.oecd-ilibrary.org.

[1646] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", *l.c.*, p. 68

[1647] U.S. Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes", *l.c.*, p. 12.

[1648] Specifically, Facebook has added "partner categories" as an additional targeting feature, which enables advertisers to target individuals based on the basis of their purchase behaviour outside the social network. See https://www.facebook-studio.com/news/item/partner-categories-a-new-self-serve-targeting-feature (last accessed 17 December 2013). See also C. Dello, "Facebook to Partner With Acxiom, Epsilon to Match Store Purchases with User Profiles – Can Facebook Ads Drive Offline Buying?", *Advertising Age*, 22 February 2013, available at http://adage.com/article/digital/facebook-partner-acxiom-epsilon-match-store-purchases-user-profiles/239967 (last accessed 7 January 2014).

[1649] K. Opshal and R. Reitman, "The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads", Electronic Frontier Foundation (EFF), 22 April 2013, available at https://www.eff.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-data-brokers-show-you-targeted-ads (last accessed 7 January 2014).

802. DATA FLOWS – Figure 4 visualizes the corresponding data flows as follows: arrow (9) represents the exchange of personal data that takes place between data brokers and social networks. It is important to note that the collection of personal data by data brokers does not necessarily involve "active" disclosure by the OSN provider (e.g., the data might simply be collected from publicly available OSN sites). Arrow (9) is bi-directional as data brokers may also indirectly reveal data about OSN users to the OSN provider (e.g., regarding their inferred interests).[1650] Arrows (7), (10) and (11) intend to illustrate that data brokers may also obtain information about individual OSN users from trackers (e.g., browsing history), application providers (e.g., app usage) or third-party website operators (e.g., purchase history).

2.6 (THIRD-PARTY) WEBSITE

803. MAIN CHARACTERISTICS – A third-party website is, as the name suggests, a website operated by an entity other than the OSN or the OSN user. Third-party websites can interact with OSNs in a variety of ways. For example, OSNs such as Facebook and MySpace allow third parties to leverage their authentication services, so that individuals can make use of their OSN credentials when accessing these websites.[1651] "Social plug-ins" are another prominent way in which third-party websites interact with OSNs. A social plug-in is a website component designed to facilitate the sharing of third-party content within OSNs. Facebook's "Like button", for example, enables users to leave positive feedback for a web page and to share it with others.[1652] Similar tools are offered by other OSNs such as Google+ ("+1"), Pinterest ("Pin it") and Linkedin ("in share").[1653]

[1650] In case of Facebook, user targeting is achieved through a matching function which has been explained as follows: a company contacts a data broker with a particular audience in mind (e.g., people interested in losing weight). The data broker then generates a list of email addresses of people it believes that belong to that audience. It then creates a cryptographic hash function for each of the email addresses of each person on the list and sends these hash functions to Facebook. Facebook then compares this list of hash functions to its own list of hash functions of email addresses belonging all Facebook users and then identifies the relevant users as being part of the target group. (K. Opshal and R. Reitman, "The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads", *l.c.*). In case of targeting based on browsing activity, mapping OSN users with the intended audience is done through a process referred to as "cookie matching". Even if data brokers do not directly share any data with Facebook other than the relevant hash functions, Facebook might still be able to glean information of the user based on what is being advertised (*Id.*).

[1651] M.N. Ko, G.P. Cheek and M. Shebab, "Social-Networks Connect Services", *Computer* 2010, Issue n° 8, IEEE Computer Society, p. 37. The Facebook platform (Facebook's API) also allows third-party sites to obtain authorization tokens from Facebook. This basically works as follows: the user first authenticates herself using Facebook as their identity provider. Next, Facebook issues a token that allows the third-party site to access the user's basic profile information. The third-party site can then request additional permissions, much in the same way as (other) application providers (*Ibid*, p. 38-39). See also *supra*; nr. 792.

[1652] G. Kontaxis, M. Polychronakis, A.D. Keromytis and E.P. Markatos, "Privacy-Preserving Social Plugins", *Proceedings of the 21st USENIX conference on Security symposium*, 2012, p. 30, available at https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final150.pdf (last accessed 8 January 2014).

[1653] By embedding social plug-ins the website operator can help increase the visibility of its webpages. It also enriches the data exchanged within OSNs, so these tools are generally considered beneficial for both

804. DATA DISCLOSURE – Despite the benefits of plug-ins, their increased presence on third-party websites has also engendered controversy. Specifically, it has been demonstrated that social plug-ins can enable OSN providers to monitor the browsing activities of its users beyond the context of the OSN.[1654] This tracking capability may exist even if the user does not actually click on the plug-in at hand. It is sufficient that the plug-in has been embedded on the website in question.[1655] Moreover, the tracking capability offered by plug-ins is not limited to OSN users. Even if an individual does not have an account with a particular OSN provider, the presence of its social plug-ins may allow it to keep track of its visits to other pages in which the plug-in has been embedded.[1656]

805. DATA FLOWS – The data flows between OSN providers and third-party websites are depicted in Figure 4 by two arrows (12): the first is a solid bi-directional arrow which represents those flows which can be easily observed or inferred by OSN users. This is the case, for example, if an OSN user decides to use its OSN credential to log-in to a third-party website or to link third-party content to his or her profile. The second arrow is a dashed arrow which is meant to capture the leakage of browsing behaviour through social-plug-ins.[1657] The term "third party" is bracketed to indicate that an OSN provider may also operate websites outside the OSN context (e.g., Google owns Youtube in addition to Google+).

2.7 OTHER OBSERVERS

806. MAIN CHARACTERISTICS – The previous sections have introduced some of the main players interacting with OSN-related data on a regular basis. An additional category of actors worth identifying is what one might refer to as "other observers". Other observers are entities who, regardless of whether or not they have a formal relationship with an OSN or its users, access data that is processed in the context of an OSN. Such access takes place regularly, and for a plethora reasons: market research,

---

website operators and OSN providers. For OSN users, the presence of social plug-ins offers convenience, as it enables them to share third-party content within their OSNs almost seamlessly. (*Id.*)

[1654] *Id.* See also A.P.C. Roosendaal, "We Are All Connected to Facebook … by Facebook!", in S. Gutwirth et al. (eds), *European Data Protection: In Good Health?*, Springer, 2012, p. 3-19. An earlier version of this paper is available on SSRN as A. Roosendaal, "Facebook tracks and traces everyone: Like this!", *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 (last accessed 8 January 2013).

[1655] *Id.*

[1656] *Id.* For a recent discussion of Facebook tracking through social plug-ins see B. Van Alsenoy, V. Verdoodt, R. Heyman, J. Ausloos, E. Wauters and G. Acar, "From social media service to advertising network - A critical analysis of Facebook's Revised Policies and Terms", v1.3, 25 August 2015, p. 89-100, available at http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf (last accessed 7 December 2015).

[1657] Dashed arrow (12) is misleading - in a way similar to arrows (7) and (9) - to the extent that tracking occurs via the browser or operating system of the user (in which case they would coincide simply with arrow (4). The decision was made to visually represent the data flows in this way in order to make clear that users can be tracked by OSN providers across websites that have their social plug-ins embedded.

student oversight, law enforcement, intelligence gathering, credit risk assessment, employee background checks, disability verification etc.

807. DATA COLLECTION AND USE – Online news outlets are brimming with reports of how schools, employers, intelligence agencies and other entities are using social media to monitor individuals' activities. For example, school administrators are often cited as reviewing social networking data for inappropriate student behaviour, such as underage drinking.[1658] Recently, a Californian high school even hired a firm to monitor public postings on social media to search for possible violence, drug use, bullying, truancy and suicidal threats.[1659] Employers are also known consult OSNs when evaluating job applicants; or to take disciplinary action towards employees (even firing) after learning about unwanted behaviour through social media data.[1660] Last, but definitely not least, recent revelations concerning intelligence operations have indicated that national security agencies also use social networking data to evaluate potential national security threats.[1661]

808. DATA FLOWS – Arrow (13) represents the data flows which take place in situations where observers access OSN-related data. It is important to note that an observer may also access these data indirectly, e.g. via a data broker or tracker (arrows (14) and (15)).[1662] Finally, it is worth underlining that the observation of OSN data is not necessarily limited to data which has been labelled as "public" according to the user's privacy settings (e.g., in case of surreptitious monitoring or co-operation with law enforcement officials).[1663]

[1658] See e.g., Associated Press, "District to monitor students MySpace pages", *NBC news*, 23 May 2006, available at http://www.nbcnews.com/id/12937962/#.Us50c7R_tGM; N. Buczek, "Schools discipline students of Internet content", 22 February 2006, http://thefire.org/index.php/article/6855.html (last accessed 9 January 2014).

[1659] M. Martinez, "California school district hires firm to monitor students' social media", *CNN*, 18 September 2013, available at http://edition.cnn.com/2013/09/14/us/california-schools-monitor-social-media (last accessed 8 January 2014).

[1660] See e.g., C.A. Ciocchetti, "The eavesdropping employer: a twenty-first century framework for employee monitoring", *Future of Privacy Forum*, 2010, p. 45 available at http://www.futureofprivacy.org/wp-content/uploads/2010/07/The_Eavesdropping_Employer_%20A_Twenty-First_Century_Framework.pdf (last accessed 9 January 2013). According to a 2009 study by Proofpoint, an internet security firm, 8 percent of companies with one thousand employees or more have terminated at least one employee for comments posted on a social networking site. See A. Ostrow, "Facebook Fired: 8% of US Companies have Sacked Social Media Miscreants", *Mashable*, 10 August 2009, available at http://mashable.com/2009/08/10/social-media-misuse (last accessed 10 January 2013).

[1661] See e.g., E. MacAskill, J. Borger, N. Hopkins, N. Davies and J. Ball, "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, Friday 21 June 2013, available at http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last accessed 9 January 2013).

[1662] For examples see K. Opshal and R. Reitman, "The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads", *l.c.*

[1663] See Facebook, "Global Government Requests Report" for an aggregate overview of the data requests received by Facebook from government officials during the first 6 months of 2013, available at https://www.facebook.com/about/government_requests (last accessed 9 January 2013).

2.8 *INFRASTRUCTURE (SERVICE) PROVIDER*

809. MAIN CHARACTERISTICS – A final category of actors which is worth mentioning are the "infrastructure (service) providers". These are the entities that operate the technical infrastructure which is necessary for OSN providers to offer their services and for OSN users to make use of the OSN. Examples include Internet Service Providers ("ISPs"), hosting service providers, device manufactures, the providers of operating systems, etc. While the role of these entities will not be discussed in detail, it is nevertheless worth noting their essential role in enabling OSN interactions.

3 ROLES

810. OUTLINE – Now that the main actors have been identified, this section will proceed to analyse their legal status under Directive 95/46/EC. Specifically, the following sections will evaluate to what extent OSN providers, OSN users, (third-party) application providers and other entities may be considered as "controllers" or "processors" within the meaning of Directive 95/46.

3.1 *OSN PROVIDER*

811. HIGH-LEVEL ANALYSIS – OSN providers are generally considered to be "controllers" within the meaning of Directive 95/46.[1664] After all, they determine both the *purposes* and *means* of their own processing activities: their *purpose* is to provide a social networking service which generates revenue. They also determine the *means* of their own processing activities: they decide about the nature of the social networking service and how it will be provided – from user registration until account deletion. In addition to those operations that are strictly necessary to provide the OSN service, the provider also decides about a range of additional processing activities; including those designed to enable targeted advertising.[1665]

[1664] See e.g. College Bescherming Persoonsgegevens, "Publicatie van Persoonsgegevens op het Internet", *CBP Richtsnoeren*, December 2007, p. 7-8; ; B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 70; Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", WP 163, 12 June 2009, p. 5; Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of controller and processor", *l.c.*, p. 21; P. Van Eecke and M. Truyens, "Privacy and social networks", *Computer Law & Security Review* 2010, Vol. 26, p. 537-538; E. Kosta, C. Kalloniatis, L. Mitrou and S. Gritzalis, "Data protection issues pertaining to social networking under EU law", *Transforming Government: People, Process and Policy* 2010, Vol. 4, No. 2, p. 196; D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *International Law & Management Review* 2010, Vol. 6, p. 131; B.J. Koops, "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice", *Tilburg Law School Legal Studies Research Paper* Series No. 08/2012, p. 10 and Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", 24 May 2013, Version 1.0, p. 10-11.

[1665] B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 70.

812. SCOPE OF CONTROL – While most would agree that OSN providers should be considered as "controllers", opinions vary as to the boundaries of their control. In certain cases, it is relatively clear whether or not an OSN provider acts is acting as a controller. For instance, few would dispute that an OSN provider acts as a controller in relation to:

- the collection and use of explicitly solicited data (e.g., information which OSN users are asked to provide when registering to the site, such as their name, age and place of residence)[1666];
- their processing of user data for purposes of targeted advertising (e.g., when analysing "behavioural data"); and
- their processing of user data designed to enhance the quality of the OSN service or to provide additional features (e.g., use of facial recognition techniques to create "tag suggests"[1667]).

813. USER-GENERATED CONTENT – While the previous examples are relatively straightforward, there are processing activities for which it is more difficult to delineate to the role of the OSN provider. A particular contentious matter is whether or not an OSN provider should be considered as a (co-)controller in relation to content shared (spontaneously) by its users. For example, should an OSN provider be considered a "controller" of the processing that takes place when its users share content with one and other (e.g., the sharing of a photograph among friends)? There are essentially four different ways in which this issue has been approached by scholars, courts and regulators, each of which will be elaborated of the following paragraphs.

814. NO CONTROL – Several authors argue that web 2.0 service providers, such as OSN providers, should not be considered as controllers in relation to user-generated content at all.[1668] After all, these entities exercise little or no influence at the moment content is being uploaded: while OSNs may encourage certain types of sharing, every user decides autonomously whether or not to share specific content. Moreover, it is argued, OSN providers cannot reasonably be expected to fulfil the obligations of controllers in relation to data shared by users (e.g., because they will not know, until after the fact, which data are being shared, about whom, etc.). Furthermore, requiring OSN providers to assume such control would have undesirable consequences, most notably for the freedom of expression of OSN users.[1669] From this perspective, it is argued that only the OSN user who decides to upload certain content should be

[1666] See also Cour d'Appel de Liège, 7ième Chambre, Bobon Benjamin / SPRL Diablo, 2008/RG/1165, 19 November 2009.
[1667] See e.g. S. Curtis, "Facebook defends using profile pictures for facial recognition", *The Telegraph*, 15 November 2013, available at http://www.telegraph.co.uk/technology/facebook/10452867/Facebook-defends-using-profile-pictures-for-facial-recognition.html.
[1668] See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *International Data Privacy Law* 2013, Vol. 3, No. 1, p. 9-10.
[1669] *Ibid*, p. 10.

considered as the controller vis-à-vis this sharing activity. The OSN provider, on the other hand, should be considered a mere "processor"[1670] or "hosting service provider"[1671].

815. PLATFORM CONTROL – Other commentators have argued that OSN providers should be considered as controllers in addition to OSN users. Specifically, they argue that the OSN provider should be considered a controller in relation to its social networking service "as a whole".[1672] Once data have been uploaded, the OSN provider proceeds to perform operations upon them which enable the actual sharing of information (e.g., storage, analysis[1673], dissemination, access control). And for these processing activities, the provider has determined the "purposes and the means" in advance, independently of the OSN users.[1674] Because the sharing of personal data among contacts is an essential component of its service, these commentators conclude that the OSN provider acts as a (co-)controller vis-à-vis the dissemination of content over its platform (even though the initiative to share this content originated from one of its users).[1675]

816. PIECEMEAL CONTROL – A third approach, which combines elements of the previous two approaches, views both OSN users and OSN providers as controllers, but each "for different combinations of data flows and purposes".[1676] In other words, both

---

[1670] See e.g. P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 537-538. Personally, I consider this interpretation is at odds with 17(3) of Directive 95/46/EC. This provision implies a willingness, on the part of the processor, to only process personal data in accordance with the instructions issued by the controller. Moreover, this provision stipulates that this willingness must be expressed in the form of a legally binding instrument. Given that many OSN providers, in practice, reserve themselves the ability to modify the nature of their services at all times, often without prior consultation of their users, I would argue that they should not be considered as "processors", but rather as separate controllers (whose "control" extends to different aspects of the processing).

[1671] See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *l.c.*, p. 5 et seq. Hosting service providers are provided with a (conditional) liability exemption under E-Commerce Directive 2000/31/EC. For purposes of conceptual clarity, the relationship between Directive 95/46/EC and E-Commerce Directive 2000/31/EC will be discussed *infra*; nrs. 874 et seq.

[1672] See B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 70.

[1673] For example, algorithmic analysis carried out by the OSN provider may determine the degree of visibility given to a particular content item. In case of Facebook's "Newsfeed", for instance, Facebook deploys an automated selection mechanism to establish relevancy of content posted by friends, which ultimately determines the degree of visibility a particular item receives. See T. Bucher, "Want to be on top? Algorithmic power and the threat of invisibility on Facebook", *New Media Society* 2012, Vol. 14, p. 1167 et seq.

[1674] See B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 71.

[1675] While this approach involves an expansive interpretation of the controller concept, these authors anticipate certain limitations as to the corresponding responsibilities and liabilities of OSN providers. For example, the indicate that OSN providers might be able to escape liability if they can demonstrate having continuously undertaken all reasonable measures to prevent the data protection violation from taking place, and to limit their effects once they have been manifested (see B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 71.)

[1676] Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 537-538.

entities might act as controllers, but each for different aspects of the processing. They each exercise control, but "at different stages" and "to different degrees".[1677] While this approach allows for greater nuance and flexibility, its practical implications are often not spelled out with great detail.

817. CONTROL UPON "ACTUAL KNOWLEDGE" – Finally, a fourth approach considers that the OSN provider may only be considered a "controller" of personal data shared over its platform once it has obtained actual knowledge of its existence. Under this approach, it is the OSN user who shares the content which is seen as the main (or "primary") controller, while the OSN provider only becomes a ("secondary") controller once it has been notified of specific personal data processing. This appears to have been the reasoning of the Italian Supreme Court in a judgement concerning *Google Video*, where the Court reasoned that

> "*[…] as long as the offense is unknown to the service provider, it cannot be regarded as the controller of the processing, because it lacks any decision-making power on the data itself, and when, instead, the provider is aware of the illegal data and is not active for its immediate removal or makes it inaccessible, however, it takes a full qualification of the data controller*".[1678]

818. ASSESSMENT – While there are notable differences among the approaches outlined above, these differences are mainly conceptual. To a large extent, the practical implications of each approach may be largely the same, depending on how one interprets the obligations resulting from the qualification of an OSN provider as a "controller". This issue will be revisited later on.[1679]

3.2 OSN USERS

819. HIGH-LEVEL ANALYSIS – Every OSN user, at least in theory, acts as a "controller" when processing data about others within an OSN.[1680] Private individuals use OSNs for

---

[1677] See Opinion 1/2010, *l.c.*, p. 22.

[1678] Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14, at paragraph 7.2. A special word of thanks is owed to Professor Giovanni Sartor for assisting me with this translation. The full text of this opinion is available at http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html (last accessed 13 February 2014).

[1679] Cf. *infra*; section 875.

[1680] B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 70; Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 5; R. Wong, "Social networking: a conceptual analysis of a data controller", *Communications Law* 2009, Vol. 14, No. 5, p. 143 et seq.; N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 102 et seq; P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 537-538; and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *l.c.*, p. 131 et seq. An individual cannot act as a controller towards his or her own data. The regulatory scheme of Directive 95/46/EC is predicated on the notion that the data controller is an entity other than the data subject him-

purposes such as social interaction, self-expression, career development and self-education. Organisations, on the other hand, typically use OSNs to further their organisational mission or corporate objectives (e.g., product promotion, membership recruitment, event planning).[1681] In both cases, the OSN user freely determines why it processes personal data relating to others. As to determining the means of the processing, OSN users generally do not have any real decision-making power. While they may have the ability to adapt some minor features or settings, they do not have any real influence as to the manner in which the processing is conducted. They either take it or leave it. But every OSN user does, as a rule, exercise the choice as to whether or not he wishes to share a particular piece of information using an OSN. In this sense OSN users still effectively determines the "means" of their processing when entrusting data about others to an OSN.[1682]

820. SCOPE OF CONTROL – The control exercised by OSN users in principle extends to any content they choose to provide and any processing operations they undertake of their own accord (i.e., without solicitation).[1683] For example, a company which uses an OSN for purposes of product promotion shall be considered a controller towards:

- any personal data that is included on the company's profile page (including its list of "connections" or "friends");
- any personal data which the company collects through the OSN (e.g., personal attributes of its connections);
- any information about individuals which the company disseminates through the OSN.[1684]

821. EXEMPTION FOR "PERSONAL USE" – The second indent of art. 3(2) provides that Directive 95/46 shall not apply to the processing of personal data "*by a natural person in the course of a purely personal or household activity*". This exemption has given rise to the following question: to what extent can OSN usage be considered a "*purely personal or household activity*"? The Court of Justice has provided further guidance regarding article 3(2), namely in the context of the *Lindqvist* case.[1685] Here, the Court considered that the exception for personal use must

---

or herself. An individual person might act as a controller of personal data relating to others, but not of his or her own personal data. See also *supra*; nr. 700.

[1681] See also Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", *l.c.*, p. 4

[1682] B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 70. One must, however, be careful not to exaggerate the decision-making power of the individual user. The controllership of the user does not extend to the SNS as a whole, but only to those processing operations for which he can actually determine the purposes and means. (*Id.*)

[1683] *Id.*

[1684] See also Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", *l.c.*, p. 3.

[1685] Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596. The facts of this case were as follows: Mrs. Lindqvist, who worked as a catechist in a local parish, had set up a number of web pages to provide

"*be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*".[1686]

822. CRITERIA FOR "PERSONAL USE" – The Court of Justice thus put forward two elements to determine whether the personal use exemption can be applied. In the first place the processing activity must be carried out "*in the course of private and family life*". Secondly, the exemption shall not apply where the data is published on the Internet and made accessible to an indefinite number of people.[1687] The first criterion suggests that private OSN users, who make use of an OSN for purposes of social interaction, should in principle be able to avail themselves of the personal use exemption. After all, social interaction is an essential component of one's private or family life.[1688] However, one must not lose track of the second element in the reasoning of the ECJ, namely that the exception shall not apply where the data is made accessible to an indefinite number of people. This implies that OSN users might not be able to invoke this exemption once the data in question passes a certain threshold of accessibility.[1689]

823. ARTICLE 29 WP – In its Opinion on social networking, the Article 29 Working Party indicated that the processing activities of private OSN users are generally covered by the personal use exemption.[1690] However, it also identified two situations in which the personal use exemption will not apply. First, the exception will not apply if the individual is acting "*on behalf of a company or association, or uses the [OSN] mainly as a*

---

information to fellow parishioners preparing for their confirmation. These pages also included information about several of her colleagues in the parish, who were referenced either by their full names or merely by their first names. In many cases telephone numbers were listed. The pages also described, "in a mildly humorous manner" the jobs held by these colleagues and their hobbies. Other information was also mentioned, such as family circumstances; and of one colleague it was stated that she had injured her foot and was working half-time for medical reasons. Mrs. Lindqvist had not obtained the consent of the individuals referenced on her web pages, nor informed them of the fact that she was mentioning personal information about them. She also had not notified the data protection authority. She was subsequently prosecuted for violation of the Swedish law on personal data.

[1686] Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paragraph 47 (emphasis added).

[1687] The Belgian Privacy Commission (CBPL), in a recommendation regarding the sharing of pictures by individuals, also touched upon the question of personal use. It considered that where images are processed for the sole purpose of distribution among a select ("definable") group of friends, family members or acquaintances, such processing could fall under the exception of personal use. As examples it mentioned the transmission of pictures via email to the participants of a family event, or the posting of such pictures on a secured website, which is only accessible to the relevant family members; and which is protected against indexing by search engines. (Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Aanbeveling uit eigen beweging inzake de verspreiding van beeldmateriaal", Aanbeveling nr. 02/2007, 28 November 2007, p. 21-22, available at www.privacycommision.be The Dutch Data Protection Authority adopted an almost identical approach shortly thereafter in its Guidance Report relating to the publication of personal data on the internet (See College Bescherming Persoonsgegevens, "Publicatie van Persoonsgegevens op het Internet", *CBP Richtsnoeren*, December 2007, p. 12–13).

[1688] B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 74.

[1689] See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 103.

[1690] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 5.

platform to advance commercial, political or charitable goals."[1691] Second, the exemption for personal use also will not apply if the individual "*takes an informed decision to extend access beyond self-selected "friends"*".[1692]

824. CONCLUSION – In conclusion, one can state that OSN users may be considered as "controllers" within the meaning of article 2(d). Organisations and companies shall in principle be subject to the same set of responsibilities as those incumbent upon controllers in any other context. In case of private individuals, the applicability of Directive 95/46/EC depends on whether or not the OSN usage falls within the remit of the personal use exemption. The implications of this outcome will be evaluated later on.[1693]

3.3 APPLICATION PROVIDERS

825. HIGH-LEVEL ANALYSIS – Third-party application providers will typically also be considered as "controllers" within the meaning of article 2(d).[1694] Similar to OSN providers, the objective of most application providers is to provide a certain service which generates revenue.[1695] The nature of this service will depend on the intended functionality of their application(s): gaming, content streaming, location sharing, crowd funding … .[1696] In this sense, application providers determine the *purposes* of the processing of user data that takes place when they provide their services. Application providers also determine the *means* of their processing: they stipulate which data will collect regarding OSN users and how these data will be subsequently processed. In addition to deciding about those activities which are necessary to deliver the app's functionality, the provider may also decide about additional processing activities; including those designed to enable targeted advertising.

826. SCOPE OF CONTROL – The "control" exercised by application providers in principle extends to any processing which takes place to support the application's functionality. It also extends to any processing undertaken by the application provider to enable targeted advertising (e.g., disclosure of a user's location to support contextual advertising).[1697] While application developers have significant freedom in deciding how

---

[1691] *Id.*
[1692] *Id.*
[1693] Cf. *infra*; nrs. 868 et seq.
[1694] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 5. See also P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 540-541.
[1695] As in the case of OSNs, many application providers derive (a portion of) their revenue from targeted advertising (so-called "in-app advertising"). Application providers may also charge money for downloads of their apps, for in-app purchases or for premium subscriptions. For an overview of the different revenue models of mobile apps see OECD, "The App Economy", *l.c.*, p. 22-26.
[1696] Cf. *supra*; nr. 791.
[1697] See also Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", WP202, 27 February 2013, p. 12available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last accessed 28 January 2014).

to organise their own processing of personal data, they are typically constrained by at least two important factors, namely the (1) terms and conditions for application developers and (2) the access control model supported by the OSN.

827. API TERMS – When collecting data related to OSN users, application providers are not entirely free in deciding how this collection shall be organized. As indicated before, many application providers obtain access to OSN data by soliciting permissions from OSN users. Once these permissions have been granted, the application provider will query the social network's Application Programming Interface (API) to make use of the delegated privileges (e.g., access profile information, post to wall).[1698] Using the API of an OSN is generally subject to a number of terms and conditions, which are stipulated by the OSN provider. As a result, application providers are in principle bound by the limitations and restrictions imposed by the API terms when soliciting, collecting and processing OSN data.[1699]

828. ACCESS CONTROL MODELS – The access rights of application providers may vary across platforms. In case of Facebook, for example, application providers are granted access to the user's "basic information" by default.[1700] This information includes user ID, name, picture, gender, locale and friend connections.[1701] Additionally, application developers may also request access to several additional permission classes (e.g., "email permissions", "extended profile properties", "extended permissions", etc.).[1702] These permissions may, for example, enable the application provider to post information on

[1698] W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 208. See also M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 1-2. A number of OSN providers, which include Google, Myspace and Yahoo united their efforts to develop a uniform social application programming interface, which is called "*OpenSocial*". The goal of this initiative is to allow application developers to offer their applications to users from various OSNs and to enable their functionality across OSNs. See W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 210. See also F. Le Borgne-Bachschmidt et al., "User-Created-Content: Supporting a participative Information Society", Final Report, 2008, p. 243, available at http://www.ivir.nl/publications/helberger/User_created_content.pdf (last accessed 28 January 2014).

[1699] For more information regarding Terms & Conditions of OSN APIs see A. Kuczerawy, "Legal and ethical analysis", *Exploiting Social Networks for Building the Future Internet of Services* (SocIoS), Deliverable D3.5, p. 21-29. While third-party application providers are bound by API terms, they in principle decide autonomously whether they wish to collect certain data via an OSN and how to use it. Although they too must "take it or leave it", they exercise a choice when deciding to collect data about individuals through an OSN API. In this sense application providers still effectively determine the "means" of their processing when collecting data about OSN users in this way.

[1700] M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 3. See also https://www.facebook.com/about/privacy/your-info-on-other (last accessed 27 January 2014).

[1701] *Id.*

[1702] *Id.* See also Facebook for developers, "Permissions Reference - Facebook Login", available at https://developers.facebook.com/docs/facebook-login/permissions (last accessed 27 January 2014).

behalf of users or to access private messages.[1703] Other OSN platforms support different access control models; which may be either more granular or more coarse-grained.[1704]

829. RELATIONSHIP TO OSN PROVIDER – Third-party application providers are in principle "separate controllers": they determine their own purposes and means for their processing of personal data.[1705] Once access has been granted, an application provider will typically collect the data and export them to its own servers for further processing.[1706] The OSN provider cannot, as a general matter, be considered as a "controller" in relation to the processing activities of third-party application developers (unless the latter are acting "on behalf of the" OSN provider). Nevertheless, the OSN provider plays an important role in ensuring that application providers (can) comply with data protection requirements (e.g., by supporting granular access to user data).

3.4 OTHER ACTORS

830. HIGH-LEVEL ANALYSIS – The previous section identified a wide range of additional actors interacting with OSN data, such as trackers, data brokers and other observers. In the interest of brevity, the legal status of each of these actors will only be discussed briefly. Generally speaking, one may start from the assumption that each of these actors will typically also be considered as "controllers" in their own right, at least insofar as their own processing activities are concerned. Only in cases where they process personal data on behalf of and in accordance with the instructions of others, may they be considered as "processors" rather than "controllers".

831. THIRD-PARTY TRACKERS – For example, a third-party tracker will in principle be considered a "controller" for its collection and analysis of data related to the web browsing behaviour of OSN users. However, it will only be considered a controller as long as it determines its own purposes and means of the processing. As indicated earlier, trackers often work on behalf of an ad network.[1707] If a tracker is working on behalf of an ad network, and only processes personal data in accordance with the instructions issued by the ad network provider, the tracker will be considered a "processor" rather than a controller. Another scenario in which a tracker might be considered a "processor" is the scenario in which the tracker processes data on behalf of the OSN provider (e.g., if

[1703] *Id.*
[1704] See also W. De Groef, D. Devries, T. Reynaert and F. Piessens, "Security and Privacy of Online Social Network Applications", *l.c.*, p. 212-213. For example, "OpenSocial" currently supports only one specific permission: allow or deny the application to access all of the user's data. However, implementers can always enhance this model in their own implementations. (*Id.*)
[1705] Cf. *supra*; nr. 825.
[1706] These servers are outside of the OSN domain, meaning they are beyond the OSN provider's direct control or supervision. (M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 2.)
[1707] Cf. *supra*; nr. 797.

the OSN provider hires a tracker to learn more about how its users navigate the OSN).[1708]

832. DATA BROKERS – Data brokers in principle act as controllers in their own right. They determine their own purposes when collecting data about individuals (e.g., collect data for purposes of profiling or predictive scoring). They also decide autonomously about how to organize this collection (e.g., which sources to consult, which technical methods to employ). While the product developed by a data broker will (eventually) be consumed by a third party, the data broker will have typically concluded its product development long before it is offered to clients.[1709]

833. OTHER OBSERVERS – Other "observers" of OSN data in principle also collect these data for their own purposes. For example, an employer who accesses the profile of a job applicant is likely to do so in order to assess the fitness of the candidate. Similarly, the intelligence agency mining OSN data in order to detect a potential threat to national security is likewise pursuing its own (statutory) objectives. In certain instances, observers may rely on the assistance of other entities to help achieve its objectives (e.g., a school may hire a private firm to monitor social network usage of its students). In these cases, the extent to which the service provider will be considered a "processor" or a "(co-)controller" will depend largely on (1) how the service provider has defined the purpose(s) of its services up front and (2) the extent to which the service provider acts in accordance with instructions issued by its customers.[1710]

4 ALLOCATION OF RESPONSIBILITY AND RISK

834. OUTLINE – The previous section analysed the legal status of each of the actors introduced in the beginning of this chapter. The purpose of this section is to detail how the main rights and obligations of each of these entities have been interpreted, in particular by the Article 29 Working Party and national regulatory authorities. In the interest of brevity, the remainder of this chapter will be focused on three actors only, namely the (1) OSN providers; (2) the OSN user and (3) application providers.

[1708] See also Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 13 (indicating that a third party provides analytics services for an application owner, without processing the data for its own purposes or sharing it across developers, it is likely to be acting as a processor).
[1709] The third party using the data broker's service will typically also be a controller in its own right, separately from the data broker.
[1710] See also B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46", *l.c.*, p. 36-37

4.1 TRANSPARENCY

835. OSN PROVIDER – As a controller, the OSN provider must provide data subjects with certain basic information regarding the processing of their personal data (articles 10-11).[1711] According to Article 29 Working party, an OSN provider should inform its users *inter alea* about:

a) the usage of their data for direct marketing purposes (e.g., the use of profile information for purposes of targeting advertisements);

b) any sharing of their data with third parties (e.g., third-party application providers);

c) any profiling to which the users might be subject, including an identification of the main data sources (e.g., personal details submitted during registration, cookies, purchase records); and

d) any use of sensitive data.[1712]

In addition to informing users about its own processing activities, the Working Party also recommends that the OSN provider:

a) provide users with adequate warnings about the privacy risks related to themselves and to others when they upload information to the OSN;

b) remind users that uploading information about other individuals might impinge upon their privacy and data protection rights; and

c) advise users that they should in principle only upload pictures or information about others with the consent of the individuals concerned.[1713]

836. APPLICATION PROVIDERS – Application providers are also obliged as controllers to provide their users with information specified in articles 10-11 of the Data Protection Directive.[1714] In practice, the provisioning of information to OSN users is often mediated through the OSN provider. Under this approach, the OSN provider communicates the

---

[1711] As a rule, each data subject must be informed of at least (1) the identity of the controller (and, if applicable, of his representative) and (2) the purposes of the processing. In addition, controllers may be required to provide the data subject with supplemental information "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject". Such additional information can refer to (1) the categories of data concerned, the recipients or categories of recipients of the data, information with regard to the existence of the right of access, the right to rectify inaccurate data, etc.

[1712] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 7.

[1713] *Id.* See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 106-107.

[1714] Prior to offering its service, the application provider will have to communicate, in one form or another: (1) its identity and contact information; (2) the precise categories of personal data (OSN and other) it will collect; (3) for which specific purposes; and (4) how users may exercise their rights. See also Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 22. For applications installed on smart devices, the Working Party has also recommended that users be informed of the retention periods of their data as well as security measures applied by the controller (*Ibid*, p. 23).

permissions requested by the application provider (e.g., access to certain categories of data). When doing so, the OSN provider may also include links to the privacy notices and terms of the application providers.[1715] In any event, the Article 29 Working Party expects OSN providers to put in place "the means to ensure" that third-party developers comply with their obligations, including the obligation to provide clear and specific information about the processing.[1716]

837. OSN USERS – If the user of an OSN is not covered by the personal use exemption, he or she is also obliged to provide data subjects with information in accordance with articles 10-11. Any use of personal data which is not already known to the data subject should be communicated to the data subject either at the moment of collection or prior to their disclosure to third parties.

838. ASSESSMENT – In theory, every actor is only obliged to ensure the transparency of processing under its control. In practice, the OSN provider is expected to do more than that. For example, the Article 29 Working Party expects OSN providers to enable third-party application providers to communicate the necessary information to data subjects. In addition, the Working Party also expects OSN providers to warn OSN users about the privacy risks related to themselves and to others when they upload information to the OSN.[1717] In both these cases, the information provisioning expected from the OSN provider concerns matters which are beyond the immediate (legal) control of the OSN provider.

4.2 LEGITIMACY

A. OSN provider

839. GROUNDS – Under Directive 95/46/EC, processing of personal data may only take place to the extent that there is a "legitimate ground" justifying the processing (article 7). There are three grounds in particular which the provider of an OSN might invoke, namely:

a) the unambiguous consent by the data subject (art. 7(a));

b) a necessity for the performance of a contract (art. 7(b)); and

[1715] Access to OSN data may also be mediated by the user rather than by the OSN (see Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 9). If that is the case, the application provider must communicate the relevant information itself before obtaining access to personal data of the OSN user.

[1716] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 8-9.

[1717] The Working Party did not specify whether these warnings were legally required, or whether they were merely a recommended "best practice". At most, an obligation to issue such warnings could be derived from the OSN provider's duty to ensure legitimacy and fairness of its own processing activities. See also *infra*; nr. 841.

c) an (overriding) legitimate interest (art. 7(f)).

840. USER DATA – For processing that is strictly necessary to provide the OSN service to its users (e.g., initial creation of profile, offering of basic functionalities), the OSN provider can in principle rely on the ground of "necessity for the performance of a contract".[1718] For a limited number of operations, the provider may also be able to rely on the "legitimate interest" ground (e.g., processing for purposes of ensuring system security).[1719] For all other processing operations, such as the use of users' personal data for advertising purposes, the provider will in principle have to obtain the unambiguous consent of its users.[1720] This consent will typically be obtained during user registration (and again, if necessary, in case of modifications to the terms of service or privacy notice).

841. THIRD-PARTY DATA – As to the processing of non-user data, the Working Party noted that

> "*Many SNS allow users to contribute data about other people, such as adding a name to a picture, rating a person, listing the "people I have met/want to meet" at events. This tagging may also identify non-members. However, the processing of such data about non-members by the SNS may only be performed if one of the criteria laid down in Article 7 of the Data Protection Directive is fulfilled."*

The Article 29 Working Party did not specify whether this obligation was directed at OSN users (who upload data relating to non-members) and/or OSN providers (who subsequently process these data). The language employed by the Working Party ("*processing … by the SNS*") seems to suggest it was directed at the latter. Given that an OSN provider will generally not have a direct relationship with non-users, it seems that article 7(f) is the only practical basis through which an OSN provider might legitimate its processing of data related to non-members.[1721]

[1718] P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 542.

[1719] *Id.* To be legitimate, the processing must respect the appropriate balance between the interests of the controller and the interests of the data subject. For more information see Article 29 Data Protection Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", WP217, 9 April 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

[1720] There are situations in which data subject consent is mandated by law, even though the OSN provider might theoretically be able to invoke another ground to legitimate the processing. For instance, article 5(3) of the E-Privacy Directive entails that the provider of an OSN must obtain the consent of its users prior to (1) the installation of any software on the device of an end-user (e.g., when offering a mobile application for the OSN); (2) any placement of cookies which are not strictly necessary to provide service (e.g., to monitor web-browsing activities outside the OSN). Consent will also de facto be necessary for the processing of user data for purposes of targeted advertising, as well as any processing of data intending to locate the geographic position of the end-user, regardless of whether it involves any storage of information on the device of the end-user. See also Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices", *l.c.*, p. 14.

[1721] Whether or not the OSN provider is required to ensure the legitimacy of its processing of non-user data in fact depends on whether or not the OSN provider is (also) considered a "controller" for these activities. See also *infra*; nrs. 881 et seq.

B. Application provider

842. GROUNDS – Similar to OSN providers, there are essentially three grounds available to application providers to legitimate their processing of personal data, namely:

(1) the unambiguous consent by the data subject (art. 7(a));

(2) a necessity for the performance of a contract (art. 7(b)); and

(3) an (overriding) legitimate interest (art. 7(f)).[1722]

843. IMPLEMENTATION – Obtaining the informed consent of OSN users shall in practice be a shared responsibility among application providers and OSN providers (at least where access to OSN data is concerned). Even though an OSN provider may not be considered as a "controller" in relation to the processing activities of application providers, it is still under an obligation to ensure the legitimacy of its own processing operations (including any disclosure to third parties). In practice, the application provider will be responsible for articulating which permissions it requires and for which purposes, while the OSN provider will de facto be responsible for communicating this information to its users and obtaining their authorizations.

C. OSN user

844. GROUNDS – OSN users should in principle only share information about others with the consent of the individuals concerned.[1723] The requirement of prior consent for dissemination of one's personal image applies regardless of whether or not the OSN user falls within the remit of the personal use exemption of article 3(2).[1724] OSN users who do

[1722] See also P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 543 and Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 14-16. 255. Similar to OSN providers, an application provider will be required to obtain consent of its users for (1) the installation of any software on the device of an end-user (e.g., when offering a mobile application) (2) any placement of cookies which are not strictly necessary to provide service (e.g., to monitor web-browsing activities outside the application environment); any use of OSN or other personal data for purpose of targeted advertising; and any processing of data intending to locate the geographic position of the end-user. Cf. *supra*; nr. 839.

[1723] *Id.* See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 106-107.

[1724] In principle, anyone seeking to record or use the image of another person must first obtain that person's consent. (D. Voorhoof and P. Valcke, *Handboek Mediarecht*, Larcier, 4e editie, 2014 p. 239-240). In legal terms, the right to control one's image is sometimes also referred to as the "right of personal portrayal" or "portrait right". The term "portrait" should be understood broadly in this context, as any reproduction of the image or likeness of a person, regardless of the technique or carrier used. (Based on P. De Hert and R. Saelens, "Recht op afbeelding", *TPR* 2009, afl. 2, 867. See also L. Dierickx, "Recht op afbeelding" in X., Reeks 'Instituut voor Familierecht en Jeugdrecht KU Leuven, nr. 89, Antwerpen, Intersentia, 2005, p. 62. On an international level, the right to control one's image is protected by several human rights instruments, such as the European Convention of Human Rights (article 8) and the International Covenant of Civil and Political Rights (article 16). B. Van Alsenoy, V. Verdoodt, R. Heyman, J. Ausloos, E. Wauters and G. Acar, *From social media service to advertising network - A critical analysis of*

not benefit from the personal use exemption may rely on their legitimate interest where public figures are concerned (article 7(f)).

D. Assessment

845. BEYOND IMMEDIATE CONTROL – As with transparency, the duty to ensure legitimacy is in principle linked to the scope of one's control. The OSN provider, however, is expected to play a proactive role in ensuring the legitimacy of processing by others. For example, the Article 29 Working Party expects OSN providers to remind OSN users that they should only upload pictures or information about others with the consent of the individuals concerned. In practice, the OSN provider also plays an important role in ensuring the legitimacy of processing by application providers by obtaining the relevant permissions from OSN users on behalf of the application provider.

4.3 DATA ACCURACY

846. BASIC PRINCIPLE – Every controller is obliged to take "every reasonable step" to ensure to ensure the accuracy of personal data under its control. The precise scope of this duty must be interpreted having regard to the purposes of the processing. For example, the standard of care for ensuring data accuracy will obviously be higher in a medical setting than in the context of OSNs.[1725]

847. OSN PROVIDER – The duty to ensure data accuracy in principle only extends to processing of personal data which is under one's control. As indicated earlier, there is some disagreement regarding the extent to which OSN providers should be considered controllers in relation to content shared spontaneously by users. If one accepts that an OSN provider should, at least to some extent, be considered as a "controller" in relation to their processing of user-generated content, the question the becomes: which measures are providers of OSNs obliged to adopt in order promote accuracy of data uploaded by their users?

848. REASONABLE MEASURES – The issue of data accuracy was not addressed by the Article 29 Working Party on online social networks. It was, however, explicitly addressed by the UK Information Commissioner's Office (ICO) in its 2013 guidance for online social networks:

Facebook's Revised Policies, 25 August 2015, v1.3 p. 86, available at https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf (last accessed 27 April 2016).

[1725] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *ICRI Working Paper Series*, Working paper 15/2013, September 2013, p. 36, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494.

"*[In] a situation where the vast majority of the site content is posted directly by third parties, the volume of third party posts is significant, site content is not moderated in advance and the site relies upon users complying with user policies and reporting problems to the site operator, we would not consider that taking 'reasonable steps' requires the operator to check every individual post for accuracy*."[1726]

In these situations, the ICO continued, it would be sufficient for the OSN provider to

a) have a *clear and prominent policy* for its users about acceptable and non-acceptable posts;

b) have clear and easy to find *procedures* in place for data subjects to dispute the accuracy of posts and ask for them to be removed; and

c) *respond to disputes* about accuracy quickly, and have procedures to remove (or suspend access to) content, at least until such time as the dispute has been settled.[1727]

849. ASSESSMENT – The approach by the ICO is clearly a pragmatic approach, which attempts to reconcile the controller's obligation to ensure data accuracy with the "open" nature of online social networks. The OSN provider is not expected to establish the accuracy of personal data prior to dissemination, but is expected to have policies which reduce the risk or, if necessary, remediate the processing of inaccurate data within the OSN.

4.4 CONFIDENTIALITY AND SECURITY

A. OSN provider

i. Privacy-friendly default settings

850. BASIC PRINCIPLE – Every controller is under a duty to ensure the security and confidentiality of processing (articles 16-17 Directive 95/46/EC).[1728] Applying notions of security and confidentiality in the context of OSNs may seem counter-intuitive at first. After all, OSNs are about sharing data rather than about keeping secrets. Nevertheless,

[1726] Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", *l.c.*, paragraph 37 (emphasis added). The ICO did indicate that it might hold otherwise in situations where data controller plays a more active role in selecting, allowing or otherwise moderating content. (*Ibid*, paragraphs 35-36.)

[1727] *Ibid*, paragraph 38.

[1728] Specifically, every controller is obliged to "implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."

OSN providers are obliged to implement appropriate measures to prevent "*unauthorized access*" as well as "*any other forms of unlawful processing*".[1729]

851. ROLE OF PRIVACY SETTINGS – In practice, accessibility of an OSN profile is determined, to greater or lesser extent, by the "privacy settings" associated with that profile.[1730] These settings enable individuals to decide, to a certain extent, about the accessibility of their OSN data (e.g., "friends only", "friends and friends-of-friends", "only me", "public", etc.). Many users wish to limit their disclosure of personal information to people they know, or perhaps even to a subset of their contacts. Other users may want to share information with the public at large. Certain types of information will of course also be more intimate then others, which may also influence preferences regarding its accessibility.

852. DEFAULT SETTINGS – Given that different OSN users may have different preferences regarding the visibility of their personal data, the question arises as to which settings should be as the default. According to the Article 29 Working Party, the OSN provider should offer default settings

> *"which allow users to freely and specifically consent to any access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties*".[1731]

In other words, the Working Party considers that access to the profile information of OSN users should be restricted to self-selected contacts (e.g., "friends", "network members") by default. OSN users should be asked for permission before access is extended to any other entity.[1732] For example, information contained in a user's profile should not be made available for indexation by (internal or external) search engines unless the user has explicitly agreed to this.[1733] By restricting access to self-selected contacts by default, OSN providers may also solidify the legitimacy and fairness of their processing activities (as users need to take affirmative action before these data are made available to other third parties).[1734]

[1729] Article 17(1) Directive 95/46/EC (emphasis added).

[1730] For a comprehensive discussion of privacy settings see J. Ausloos, E. Lievens, Els Kindt and J. Dumortier, "Guidelines for privacy-friendly default settings", *SPION*, Deliverable D6.4, 2012, available at www.spion.me.

[1731] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 7.

[1732] This includes access to personal data by application providers, including when this application has not been downloaded by the OSN user herself, but rather by one of her contacts.

[1733] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 7.

[1734] See also J. Ausloos, E. Lievens, Els Kindt and J. Dumortier, "Guidelines for privacy-friendly default settings", *l.c.*, p. 30 et seq. Similar reasoning regarding the controller's duty to ensure the confidentiality and security of processing can also be found in the opinions of the Article 29 Working Party regarding applications for smart devices and location-based services. See in particular Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 11 and 15 and Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices", *l.c.*, p. 13-14.

ii. Access by third-party apps

853. LAYERED ACCESS – The Article 29 Working Party considers that OSN providers should support "layered access", so that third-party application providers can limit their collection of personal data.[1735] The OSN provider is also obliged, as part of its security obligation, to ensure that application providers do not obtain access to more data than has been authorized by users.[1736]

854. MEANINGFUL CONSENT – Technically speaking, obtaining access to data about an OSN user constitutes not only a collection by the recipient, but also a disclosure by the OSN provider.[1737] As a result, OSN providers are obliged take reasonable measures to ensure that meaningful consent is obtained from their users for the disclosure of personal data to application developers.[1738] For example, the OSN provider could require its application providers to use a standardised privacy notice. At a minimum, the OSN provider should ensure that the requested permissions and (references to) privacy notices are displayed in a prominent way.

855. COUNTERING MISUSE – The OSN provider is obliged to deploy appropriate measures to detect and remedy apparent misuse by application providers (e.g., complaint handling mechanisms, use of spam detection tools)[1739].

856. ASSESSMENT – OSN providers are obliged to ensure the confidentiality and security of their users' data. In practice, this requires the OSN provider to design its system in such a way that it enables and promotes compliance by third party application providers - even if the subsequent processing activities by those third parties are beyond its (legal) control.

857. DUTY OF CARE – An interesting question to consider is whether OSN providers are under a duty to ensure that data is only being shared with "reliable" entities.[1740] OSNs generally tend to dissociate themselves from application providers, who they consider as "third parties".[1741] They typically disclaim any and all responsibility for

---

[1735] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 9.
[1736] See also Data Protection Commissioner, "Report of Audit – Facebook Ireland Ltd.", *l.c.*, p. 88.
[1737] E. Denham (Assistant Privacy Commissioner of Canada), "Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act, 2009, p. 52, available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.
[1738] See also E. Denham, "Report of Findings - CIPPIC v. Facebook Inc.", *l.c.*, p. 3 and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *l.c.*, p. 137.
[1739] See Data Protection Commissioner, "Report of Audit – Facebook Ireland Ltd.", *l.c.*, p. 89-97. See also Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 20-21.
[1740] F. Le Borgne-Bachschmidt et al., "User-Created-Content: Supporting a participative Information Society", *l.c.*, p. 243-244.
[1741] P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 541.

actions undertaken by these third parties.[1742] Nevertheless, one could argue that OSN providers have a basic duty of care to establish that the recipients of the data under their control are in fact trustworthy (i.e. likely to process it in a lawful manner).[1743] Opponents will argue that this interpretation is excessive, and that it is sufficient for the OSN provider to assume responsibility for its own operations (i.e., the boundaries of its control establish the boundaries of its obligations).

858. DECEPTIVE PRACTICES – Finally, it is worth noting that the duties of OSN providers in relation to third party apps may also depend on how these apps are presented to users. In 2008, Facebook introduced a "verified apps" program, to which application developers could apply on a voluntary basis. If approved, the application would receive a "Facebook-verified badge" as well as increased distribution.[1744] Facebook also implied that verified applications were "*secure, respectful and transparent*".[1745] In 2012, the US Federal Trade Commission issued a complaint alleging that Facebook in fact did not take any steps to verify the security practices of a Verified Application provider ("*beyond such steps as it may have taken regarding any other application*").[1746] The complaint eventually resulted in a decision which ordered that Facebook refrain from misrepresenting "*the steps it takes or has taken to verify the privacy or security protections that any third party provides*".[1747]

B. Application provider

859. SEPARATE OBLIGATION – Application providers are also obliged to ensure the security and confidentiality of the personal data which they process. In practice, many application providers will export (a subset of) the data they collect from OSN providers

---

[1742] See also F. Le Borgne-Bachschmidt et al., "User-Created-Content: Supporting a participative Information Society", *l.c.*, p. 243-244 and E. Denham (Assistant Privacy Commissioner of Canada), "Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act", *l.c.* paragraphs 166 et seq.

[1743] F. Le Borgne-Bachschmidt et al., "User-Created-Content: Supporting a participative Information Society", *l.c.*, p. 244. These authors argue that such an obligation can be derived from article 6(1) of Directive 95/46, which requires that personal data must be processed "fairly and lawfully". They draw further support for this proposition through a comparison with article 17(2) of the Directive, which provides for a duty of care when choosing a processor who will process personal data on behalf of a controller (*Id.*) An alternative way of phrasing this argument would be to say that the OSN provider acts as a "custodian" (or "steward") of data entrusted by its users, who as a result has a certain duty of care before releasing data to third parties.

[1744] E. Denham, "Report of Findings - CIPPIC v. Facebook Inc.", *l.c.*, p. 43.

[1745] United States Federal Trade Commission (FTC), *In the matter of Facebook Inc. - Complaint*, Docket No. C-4365, 2012, p. 15, available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf (last accessed 4 February 2014).

[1746] *Id.*

[1747] United States Federal Trade Commission (FTC), *In the matter of Facebook Inc. – Decision and Order*, Docket No. C-4365, 2012, p. 4, available at http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (last accessed 4 February 2014).

to their own servers for further processing.[1748] This means that they alone shall be capable of (and responsible for) ensuring security of processing. In its Opinion on apps for smart devices, the Article 29 Working Party highlighted a number of security considerations for app developers, including:

a) measures to protect data both in transit and at rest;

b) measures to prevent "buffer overflow" or "injection" attacks;

c) use of low entropy app-specific or temporary device identifiers;

d) use of secure identification and authentication mechanisms.[1749]

C. OSN user

860. LIMITED CONTROL – OSN users have very little control over the security of data processed within the OSN – even if they formally act as a controller for their own processing operations and fall outside the scope of the personal use exemption. The OSN user must therefore carefully consider whether the security afforded by the OSN provider are sufficient in light of the risks presented by the processing. If this is not the case, the OSN user should refrain from uploading the data in question.

4.5 DATA SUBJECT RIGHTS

A. OSN Provider

861. PROBLEM STATEMENT – As a controller, the provider of an OSN must accommodate the exercise of data subject rights. The exercise of these rights vis-à-vis an OSN provider is relatively straightforward in cases where the OSN provider has actively solicited the information at issue. Similarly, it seems only natural that the OSN provider accommodate data subject rights in relation to processing activities for which it alone has determined the purposes and means (e.g. use of profile information for advertising purposes, use facial recognition to develop tag suggests). As indicated earlier, however, much of the data shared on OSNs are not actively solicited by the OSN provider, but instead shared spontaneously by its users. An interesting question to consider therefore is whether OSN providers are also obliged to accommodate the exercise of data subject rights in relation to such content. For example, should an individual have a right to ask an OSN provider to take down a photograph posted by one of its users?

[1748] These servers are outside of the OSN domain, meaning they are beyond the OSN provider's direct control or supervision. (M. Huber, M. Mulazzani, S. Schrittwieser, E.R. Weippl, "AppInspect – Large-scale Evaluation of Social Apps", *l.c.*, p. 2.)

[1749] Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 18-20.

862. RELATION TO CONTROL – In principle, individuals can only exercise their rights as data subjects vis-à-vis the "controller" of the processing. The previous sections have made clear that OSNs may involve a multitude of actors, who may each be in "control" of different (aspects of different) processing operations. In principle, each entity is only responsible for those aspects under its own control, i.e. for which determines the "purposes and means" of the processing.

863. ARTICLE 29 WP – While the initiative to share content typically stems from an OSN user (who may therefore be considered as the "primary" controller), most regulators seem to agree that OSN providers should put in place a mechanism to enable individuals to exercise their data subject rights directly towards the OSN provider.[1750] For example, in its Opinion on online social networks, the Article 29 Working Party considered that

> *"Access and rectification rights of users are not limited to the users of the service but to any natural person whose data are processed. Members and non-members of SNS must have a means to exercise their right of access, correction and deletion. The homepage of SNS sites should clearly refer to the existence of a "complaint handling office" set up by the SNS provider to deal with data protection and privacy issues and complaints by both members and non-members."*[1751]

Although it is not stated explicitly as such, the quoted text suggests that OSN providers have a duty to accommodate data subject rights in relation to *any* personal data they process. This would imply that individuals can also exercise their rights as data subjects in relation to content shared by OSN users, seeing as these data are also processed by the OSN provider. This interpretation is also in line with guidance issued by national regulators, such as the Dutch Data Protection Authority[1752] and the UK Information Commissioner's Office[1753].[1754]

864. OPEN ISSUES – While the guidance issued by the Working Party was most welcome, it refrained from offering any additional guidance as to how OSN providers should actually deal with the exercise of data subject rights. Should they immediately

---

[1750] As indicated earlier, there a number of scholars who have argued that OSN providers (or the providers of similar services) should not be considered as "controllers" in relation to the content shared via their platforms. As a result, these authors question the duty of these platform providers to accommodate data subject rights vis-à-vis user-generated content. Van Eecke and Truyens, for example, argue that an OSN provider should be considered as a mere processor in relation to content shared by users. In their view, only users should responsible for accommodating data subject rights. See P. Van Eecke and M. Truyens, "Privacy and Social Networks", *l.c.*, p. 539 and p. 543.

[1751] Article 29 Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 11 (emphasis added).

[1752] College Bescherming Persoonsgegevens, "Publicatie van Persoonsgegevens op het Internet", *l.c.*, p. 42.

[1753] Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", *l.c.*, p. 14.

[1754] See also R. Wong, "Social networking: a conceptual analysis of a data controller", *Communications Law* 2009, Vol. 14, No. 5, p. 148. For an example of a recent order issued by the Italian Data Protection Authority see Garante per la protezione dei dati personali, Provvedimento dell'11 febbraio 2016 [doc. web n. 4833448], 11 Feburary 2016, available at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4833448 (last accessed 12 May 2016).

remove any content upon request? Should they query the OSN user from whom the content originated? Should the latter be able to contest the data subject's complaint? The potential negative implications of the lack of clear guidance in this respect will be revisited later on.

B. Application provider

865. WITHDRAWAL OF CONSENT – Application providers must enable users to exercise their rights as data subjects provided by articles 12 and 14.[1755] Application users should also be provided the ability to withdraw their consent at any time.[1756] Given their role in facilitating access to OSN data, OSN providers may also be expected to offer tools which allow OSN users to discontinue access to their profile data (unless such access is already limited by default, e.g., to moments at which the application is being used by the OSN users).[1757]

C. User

866. LIMITED CONTROL – OSN users who do not fall under the personal use exemption are obliged to accommodate data subject rights. In practice, every OSN user can only administrate its own profile page. It has little or no ability to influence the subsequent use of data by the OSN provider once it has been uploaded. The OSN user must therefore carefully consider whether the subsequent processing by the OSN provider is compatible with the purposes for which the OSN user collected the data. If this is not the case, the OSN user should in principle refrain from uploading the data in question (or, if the data have already been uploaded, remove it as soon as soon as the individual concerned objects).

[1755] The Article 29 Working Party recommends that application providers allow their users to exercise these rights by means of a secure online access tool. (*Ibid*, p. 24).
[1756] *Ibid*, p. 25.
[1757] While not mentioned explicitly by the Article 29 Working Party in its opinion on online social networking, it reached a similar conclusion in its opinion related to apps on smart devices. See Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 25.

5 EVALUATION

867. OUTLINE – For the most part, regulators and scholars have been able to reconcile the regulatory framework of Directive 95/46 with new social networking realities. But there are also instances in which this framework is beginning to show its limits. There are three areas in particular which merit further consideration, namely (1) the scope of the personal use exemption; (2) the exercise of data subject rights towards user-generated content; and (3) the responsibilities of platform providers.

5.1 SCOPE OF THE PERSONAL USE EXEMPTION

868. OSN USERS AS CONTROLLERS – Section 3.2 analysed the extent to which a user of an OSN may be considered as a "controller" within the meaning of article 2(d). The conclusion was that every OSN user, at least in theory, acts as a "controller" when processing data relating to others. This implies that OSN users shall in principle be subject to the same requirements and obligations as other controllers, unless they can avail themselves from one of the exemptions recognized by Directive 95/46/EC.

869. PERSONAL USE? – In its Opinion on social networking, the Working Party considered that the processing activities of private OSN users will generally be covered by the personal use exemption.[1758] Since then, several commentators have contested this view; arguing that in practice there are many situations in which the exemption is inapplicable.[1759] First, it appears to be common ground that the exemption does not apply in situations where data are made accessible to "an indefinite number of people".[1760] As a result, OSN users with "public" profiles will almost certainly fall outside the scope of article 3(2). Even if a profile is set to "private", however, it is quite possible that the information is still *de facto* accessible to an "indefinite" number of people (e.g., due to access by "friends-of-friends").[1761] Second, a substantial share of individuals does

[1758] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", *l.c.*, p. 5.

[1759] See e.g. P. Van Eecke and M. Truyens, "Privacy and Social Networks", l.c., p. 540; N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 101 et seq. and D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *l.c.*, p. 147 et seq. Even before Opinion 5/2009, several authors considered it likely that a substantial number of OSN users might not be able to benefit from the personal use exemption. See e.g. R. Wong, "Social Networking: Anybody is a Data Controller!", (last revised) 2008, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668 and B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 75.

[1760] See also *supra*; nrs. 821 et seq.

[1761] Previous research has indicated that many users set a relatively low threshold for deciding whether to accept someone as a "friend" (See e.g. R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks", in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (WPES'05), Virginia, 2005. p. 73 and d. boyd, "Friendster and Publicly Articulated Social Networks", in *Conference on Human Factors and Computing Systems* (CHI 2004), Vienna, ACM, April 24–29, 2004, p. 1280. Contra: R. Goettke and J. Christiana, "Privacy and Online Social Networking Websites", Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May

not only (or not exclusively) use OSNs for personal purposes, but also for professional networking or for political, commercial or charitable ends.[1762] Given that the exemption of article 3(2) only applies to "purely" personal or household activities, those users would find themselves outside its protective remit.

870. IMPLICATIONS – In cases where the personal use exemption cannot be applied, the OSN user in question shall in principle be subject to the same requirements as those incumbent upon controllers in any other context.[1763] This outcome is warranted where organisations are concerned, who make use of OSNs to realize their commercial, political or other objectives. This outcome is more problematic, however, where private individuals are concerned. If an OSN user is subject to data protection law, it implies, inter alia, that this OSN user is required to ensure:

(1) the legitimacy of processing (e.g., by asking for consent before posting data relating to others);

(2) transparency of processing (e.g., by notifying the individuals concerned of the fact that information about them is now included on an OSN profile);

(3) respect for the data quality principles such as fairness, proportionality, finality and accuracy (e.g., by refraining from posting erroneous statements);

(4) that data subjects have the ability to exercise his rights towards the processing (i.e. right of access, rectification, erasure or blocking);

(5) the confidentiality and security of processing (e.g., by restricting access to individuals from the same community);

(6) that, where required, notification to national supervisory authorities is performed.

871. ASSESSMENT – At first glance, it seems as if a number of these requirements could be applied to private individuals in a reasonable way. For example, many would agree that "friends" should refrain from uploading pictures of one and other before

---

14, 2007. http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf). Given that many profiles are accessible also to "friends of friends", even a profile with a relatively low number contacts may in practice have an extremely large audience. According to a recent study by the Pew Research Institute, the *median* Facebook user can reach *31,170* people through their "*friends-of-friends*". (K. N. Hampton, L.S. Goulet, C. Marlow and L. Rainie, "Why Facebook users get more than they give", *Pew Research Center's Internet & American Life Project*, 2012, p. 5, available at http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Facebook%20users_2.3.12.pdf). See also M. Isaac, "On Facebook, There's No Privacy Setting for Your Friends' Bad Judgment", *All things D*, 26 December 2012, available at http://allthingsd.com/20121226/on-facebook-theres-no-privacy-setting-for-your-friends-bad-judgment/ (last accessed 10 February). Finally, regarding the "blurry-edged" nature of social networks see also L. Gelman, "Privacy, Free Speech, and "Blurry-Edged" Social Networks", *Boston College Law Review* 2009, vol. 50, in particular at p. 1326 et seq.

[1762] N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 103.

[1763] Cf. *supra*; *supra*; nrs. 821 et seq.

checking whether it's ok.[1764] Or that they should not post inaccurate or harmful statements about others, regardless of whether or not their profile is set to "private". For other data protection requirements, however, there appears to be a clear mismatch between legal provisions and OSN practices. For example, how does one interpret the requirement of not keeping personal data in identifiable form for longer than is necessary (art. 6(1)e) in relation to OSN users? Is it possible to determine a reasonable time-span as to how long a user should be allowed to maintain a picture or remark relating to another person on his profile page? Should we be requiring individuals to make such a determination? Another problematic provision is the controller's duty to inform.[1765] Should OSN users be required to formally notify their peers of (1) their identities; (2) the purposes of the processing of their personal data as well as (3) the (categories of) recipients concerned? Or is it sufficient if these things are understood implicitly, as a result of prevailing social norms and common OSN practices?

872. DEPENDENCIES – It is also worth noting that there are a number of controller obligations with which the OSN user cannot comply without co-operation of the OSN provider. Let us assume, for instance, that a data subject exercises his or her right to erasure towards a profile owner. Arguably, the latter would (more often than not) be under an obligation to remove this information immediately. However, what happens when the OSN provider retains these data for a longer period of time, in accordance with the terms and conditions of its service? Private OSN users have limited powers of negotiation in relation to the terms specified by the OSN provider.[1766] This imbalance does not, however, excuse OSN users from their compliance obligations. Is it reasonable to ask individuals to take such considerations into account when deciding whether or not to use an OSN?

873. A PRAGMATIC APPROACH – The mismatch between data protection requirements and OSN practices has led several authors to advocate for a pragmatic approach.[1767] Rather than rigid adherence to the provisions of the Directive 95/46/EC, they argue, OSN providers and OSN users should share the burdens of compliance in light of their respective roles. The implementation of this approach corresponds, by and large, to the recommendations issued by the Article 29 Working Party in its Opinion on online social networks. For example, the Working Party already recommended that OSN providers make users aware of the privacy risks involved in uploading information related to others, and that they should obtain their consent before doing so. The use of privacy-friendly default settings may similarly be viewed as an example of a technical

[1764] See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 104. Others may find it perfectly acceptable (and even enjoyable) to find themselves "tagged" unexpectedly in a picture uploaded by a shared contact.
[1765] See also D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *l.c.*, p. 132.
[1766] *Id.*
[1767] N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 105 et seq.

measure that supports users when they exercise their responsibilities as "controllers".[1768] While this pragmatic approach seems reasonable (and perhaps even commendable as a matter of practice), one also cannot help but wonder whether the framework of Directive 95/46/EC is being stretched too far beyond its intended scope of application.

5.2 *CONTROL OVER USER-GENERATED CONTENT*

874. DO OSN PROVIDERS "CONTROL" UGC? – Opinions vary on the extent to which OSN providers should be considered as "controllers" in relation to user-generated content.[1769] Some argue that OSN providers should be considered as controllers given the nature of their service. Others consider an OSN provider as a mere "processor", who stores and disseminates content on behalf of its users. Yet others would argue that OSN providers should instead be treated as "hosts" within the meaning of Directive 2000/31/EC.[1770]

875. PRACTICAL IMPLICATIONS – While the differences among the approaches outlined above are considerable, they are mainly conceptual. The practical implications of each approach may be largely the same, depending on how one interprets the obligations resulting from the qualification of an OSN provider as a "controller". For example, those who consider OSN providers as "controllers", typically do not expect them to proactively assess the legality of every item shared by users.[1771] The "reasonable measures", which may be expected from OSN providers under this approach, are typically limited to complaint handling once an incident has occurred. [1772] This outcome is quite similar to the "notice-and-take down" mechanisms for hosts resulting from Directive 2000/31/EC. The practical implications in the context of OSNs should therefore not be overstated.[1773] From a policy perspective, however, it is worth considering whether or not this approach should be formalized (e.g., by formally declaring the exemptions contained in the E-Commerce Directive applicable to matters involving data protection).[1774]

876. BENEFITS – Allowing individuals to exercise their rights vis-à-vis OSN providers offers certain advantages, at least from a privacy perspective. In practice, an individual

---

[1768] *Id.*

[1769] Cf. *supra*; nrs. 812 et seq.

[1770] See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *l.c.*, p. 5 et seq.

[1771] See e.g., B. Van Alsenoy, J. Ballet and A. Kuczerawy, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 71; Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", *l.c.*, paragraphs 35-37. See also *supra*; nr. 848.

[1772] *Id.*

[1773] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 61-62.

[1774] The relationship between Directive 95/46/EC and E-Commerce Directive 2000/31/EC will be discussed *infra*; nrs. 1151 et seq.

may encounter several difficulties when trying to exercise her rights towards an OSN user. First off, the OSN user may be acting within the scope of the personal use exemption, which means that they are not obliged to consider data subject rights. Even if the OSN user is acting beyond the scope of article 3(2), he or she might still refuse to take down the content at issue (e.g., by arguing that its interests in sharing the content supersede the privacy interests of the person concerned). Enforcement can be quite difficult and costly, particularly where the defendant resides in a foreign jurisdiction or if the real identity of the OSN user is concealed.[1775] For each of these reasons, the individual concerned may want to turn to the OSN provider for help.[1776]

877. RISKS OF OVER-BLOCKING – While the assistance of OSN providers can offer certain benefits, it also entails certain risks. Without appropriate safeguards, there is a risk that OSN providers might take down content simply because they receive a complaint. After all, the OSN provider may need to decide swiftly about removing or blocking the content at issue in order to exonerate itself from potential liability.[1777] This could easily lead to preventive over-blocking of entirely legitimate content.[1778] Several organisations, including the Council of Europe, have expressed concerns about possible "chilling effects" of such "notice-and-take down" procedures upon individuals' freedom of expression.[1779]

878. NO DUE PROCESS – Another concern is that the OSN user from whom the content originated may not even be made aware of the fact that someone objected to it. Or if aware, he or she may not be given the opportunity to defend the use of that content

---

[1775] See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 108.

[1776] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 5.

[1777] The liability exposure of OSN providers may stem either from the consideration that (1) the OSN provider is acting as controller in relation to the content at issue; (2) failure to remove the content at issue falls short of a reasonable standard of care (liability in tort); or (3) failure to act expeditiously results in loss of a liability exemption (e.g., the liability exemption accorded to "hosting service providers" under E-Commerce Directive 2000/31/EC).

[1778] Similar concerns have been expressed in relation to so-called "notice-and-take down" procedures, such as the ones resulting from EU E-Commerce Directive 2000/31/EC. See also C. Ahlert, C. Marsden and C. Yung, "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation" ("Mystery Shopper") at http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf (last accessed 28 April 2016). For a more detailed discussion of notice-and-take down mechanisms, as well as their relationship to Directive 95/46/EC, see also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 58 et seq.

[1779] In its document "Declaration on freedom of communications on the Internet", the Council of Europe stated that: *"Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability".* (Council of Europe (Council of Ministers), Declaration on freedom of communications on the Internet, 28 May 2003, available at: http://www.coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.)

before it is removed. This is at odds with the principles of due process, according to which one should be given the opportunity to be heard before being deprived of one's rights.[1780]

879. COMPLEXITY – Finally, there is also the issue of complexity: assessing the legitimacy of a complaint may be difficult in practice.[1781] The evaluation of subjective rights such as the right to privacy is often a delicate exercise; one which is traditionally bestowed upon courts or regulators (rather than upon private actors). Furthermore, perceptions of privacy may also be strongly influenced by cultural factors, which may make it difficult to develop a uniform approach (particularly for OSN providers which have an international user base).

880. BALANCING OF RIGHTS – Over-compliance with removal requests poses a significant threat to freedom of expression. This problem is not, however, limited to matters concerning data protection.[1782] While certain types of content can more readily be identified as "illegal" or "inappropriate", an evaluation will always be necessary.[1783] A number of measures could be devised to help mitigate the risk of unjustified take-downs. For example, one might grant an OSN provider some leeway, by saying that it shall only be responsible for removing if it is sufficiently clear that the interests of the data subject outweigh the interests of others. Furthermore, the OSN user from whom the content originated should in principle be offered the opportunity to defend their use of the content. It is beyond the scope of this thesis, however, to investigate this matter in greater depth. Further research is necessary to determine whether additional measures can help promote a better balance between the competing interests of privacy and freedom expression.

[1780] See also A. Kuczerawy and J. Ausloos, "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling", *CiTiP Working Paper Series* 2015, p. 13, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2669471.

[1781] See also Lievens E., *Protecting Children in the Digital Era – the Use of Alternative Regulatory Instruments*, Martinus Nijhoff Publishers, International Studies in Human Rights, Leiden, 2010, p. 360 (with reference Montéro E., "La responsabilité des prestataires intermediaries sur les réseaux", in: Montéro E. (ed.), *Le commerce electronique europeen sur les rails?*, *Cahiers du CRID*, Brussel, Bruylant, 2001, 289-290.)

[1782] See also B. Van Alsenoy , A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 69, with reference to the First Report on the Application of Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21 November 2003; Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf; Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11 January 2012 SEC(2011) 1641 final.

[1783] *Id.*

5.3 *RESPONSIBILITIES OF PLATFORM PROVIDERS*

881. PLATFORM RESPONSIBILITY – The provider of an OSN is uniquely placed to influence the processing of personal data that takes place on its platform. It can influence behaviour both by setting policies for acceptable use (e.g., do not collect user data without consent) and by administering these policies (e.g., by blocking apps containing malware). The previous sections have shown that OSN providers are expected to implement a number of privacy-preserving measures in their role as platform providers. This "platform responsibility"[1784] of OSN providers is not only a corporate social responsibility, it is also part of their fiduciary obligations as data controllers.

882. FIDUCIARY OBLIGATIONS – Every controller has certain fiduciary obligations in relation to the personal data which have been entrusted to it. For example, every controller must in principle assess the legitimacy of an access request before making data available to third parties.[1785] From a legal perspective, this obligation stems from the fact that every "access" by a third party is also a "disclosure" by the holder of the data, i.e. a processing operation for which the controller is legally responsible.[1786] Through regulatory guidance, the Article 29 Working Party and national authorities have attempted to clarify the fiduciary duties of OSN providers in relation to third-party applications. Specifically, the OSN provider who enables access by third-party applications is obliged to:

a) ensure that access by third-party applications is transparent to users;

b) support layered access, so that the collection of personal data by third-party apps can be limited to that which is necessary;

c) ensure that application providers obtain meaningful consent from OSN users;

d) implement privacy-friendly default settings, in order to reduce the risk of unlawful processing by third parties;

e) remove or block of apps that compromise the privacy or security of OSN users;

[1784] The concept of "platform responsibility" aims to further stimulate respect of human rights by private companies that manage online platforms. Building on Ruggie's framework "Protect, Respect and Remedy", platform responsibility begins from the finding that online platform providers (such as OSN providers) have the ability to impact different human rights, notably freedom of expression and privacy. For more information see the website of the Dynamic Coalition on Platform Responsibility: http://platformresponsibility.info (last accessed 11 December 2015). See also J. Ruggie, "Protect, Respect and Remedy - A Framework for Business and Human Rights", Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *innovations* (a United Nations publication), 2008, p. 189-212.

[1785] An obvious exception to this rule is of course personal data which are legitimately made publically available, e.g. through a publically accessible website.

[1786] See also *supra*; nr. 854.

f) provide tools which allow OSN users to discontinue the access by application providers to their profile data.[1787]

883. BEYOND CONTROL – In principle, every actor is only responsible for processing under its "control", i.e., for which it determines the purposes and means. In practice, the responsibilities of the OSN provider extend further than its own processing activities. For example, the use of malware technology by a third-party application provider is not under the "control" of the OSN provider. Nevertheless, regulators consider it the duty of OSN providers to block or remove misbehaving apps.[1788] While there is a clear legal foundation for this obligation (i.e., the duty implement appropriate measures "to prevent other forms of unlawful processing"), it also expands the scope of responsibilities of OSN providers to areas which are beyond their immediate (legal) control.[1789]

884. CONTEXT, ROLE AND ABILITY TO ACT – The obligations imposed upon OSN providers in their role as platform providers are consistent with the second principle of the OECD Recommendation on Digital Security Risk Management. The second principle ("responsibility") stipulates that all stakeholders should take responsibility for the management of digital security risks "*based on their roles, the context and their ability to act*".[1790] Data protection authorities simply expect more from OSN providers in areas where they are best placed to act, even if not every subsequent processing operation is under their control. Conversely, data protection authorities are seemingly willing to relax the obligations in other areas, where the OSN provider is less suited to act. For example, the ICO has interpreted the OSN provider's duty to ensure data accuracy in a

[1787] While not mentioned explicitly by the Article 29 Working Party in its opinion on online social networking, it reached a similar conclusion in its opinion related to apps on smart devices. See Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. 25.

[1788] See e.g. Data Protection Commissioner, "Report of Audit – Facebook Ireland Ltd.", *l.c.*, p. 97. A similar approach was adopted by WP29 in relation to providers of mobile operating systems and app stores (Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", *l.c.*, p. p11 and p. 20) For an overview of security measures which app store providers can implement see also M. Decker and G. Hogben, "Appstore security: 5 lines of defence against malware", ENISA, 2011, 20 p., available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware. Another example is the recommendation of the Article 29 Working Party to warn OSN users about the privacy risks related to themselves and to others when they upload information to the OSN. Strictly speaking, the decision to upload a particular piece of information is beyond the immediate (legal) control of the OSN provider. Nevertheless, the OSN provider is uniquely placed to educate users and raise awareness about privacy issues involved in sharing information relating to others.

[1789] For an in-depth discussion of the normative foundation of the responsibility of internet intermediaries see M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", University of Hong Kong Faculty of Law Research Paper No. 2015/45, 55 p., available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2683301 (last accessed 16 January 2016).

[1790] See the second principle of the OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2015, accessible at http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

pragmatic way, basically limiting its duties to ex post intervention in case of a dispute.[1791]

[1791] Cf. *supra*; nr. 848.

Chapter 4 CLOUD COMPUTING

1 INTRODUCTION

885. WHAT IS CLOUD COMPUTING? – Cloud computing has been defined in many ways. Most commonly cited is the definition of the U.S. National Institute for Standards and Technology (NIST), which describes cloud computing as

> *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[1792]

The European Network and Information Security Agency (ENISA) defines cloud computing in slightly more neutral terms, as

> "*an on-demand service model for IT provision, often based on virtualization and distributed computing technologies.*"[1793]

886. KEY CHARACTERISTICS – Cloud computing involves the remote consumption of IT resources via a network (e.g., the Internet).[1794] Not every Internet application, however, is deemed worthy of the label of cloud computing.[1795] Most authors also consider "elasticity" and "measured service" as defining characteristics of cloud computing.[1796] Cloud providers typically allow customers to expand or decrease their

---

[1792] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, National Institute of Standards and Technology (NIST), May 2012, p. 2-1. A draft version of the influential definition was already released in 2009 (http://www.nist.gov/itl/csd/cloud-102511.cfm).

[1793] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 14, available at https://www.enisa.europa.eu/events/speak/cloud.jpg/view (last accessed 20 December 2015).

[1794] While most cloud computing services are delivered via the Internet, cloud computing services may also be offered across a local or private network. (Information Commissioner's Office (ICO), "Guidance on the use of cloud computing", v1.1, 2 October 2012, p. 4, available at https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf (last accessed 20 December 2015).

[1795] D. Bigo a.o., "Fighting cyber crime and protecting privacy in the cloud", Study for the European Parliament, Committee on Civil Liberties, Justice and Home Affairs, PE 462.509, 2012, p. 14. It should be noted, however, that certain definitions of cloud computing are so broad that they could potentially include any type of service accessed via the internet. Early critics of the computing hype also eagerly pointed out that, after all is said and done, cloud computing is nothing more than "a computer attached to a network". See R. Leenes, "Who Controls the Cloud?", *Revista D'Internet, Dret I Política (IDP)* 2010, nr. 11, p. 2 (quoting Larry Ellison, CEO of Oracle).

[1796] See e.g., L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1; Information Commissioner's Office (ICO), *Guidance on the use of cloud computing*, *o.c.*, p. 4 and S.Y. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *Computer, Law & Security Review* 2012, Vol. 28, p. 663.

resource consumption almost instantaneously, on a "pay as you go" basis.[1797] Finally, cloud services (especially infrastructure services) are often presented in a "virtualised" manner: providers dynamically assign and reassign resources from a pool which are shared as fungible resources with other customers.[1798]

887. BENEFITS – When using cloud computing, the customer externalises part of its IT infrastructure and associated maintenance.[1799] Instead of purchasing his own hardware and software, the customer relies on the services of the cloud provider. Because customers normally pay by usage, they can avoid large upfront costs which may otherwise be necessary to set up and operate sophisticated computing equipment.[1800] Moreover, customers can scale up or down rapidly as their needs increase or decrease.[1801] Put differently, cloud computing promises "computing power on demand", with limited or no expense beyond actual consumption.[1802] Providers, in turn, are able to leverage economies of scale, by pooling their resources and reaching large volumes of customers with relatively low overhead.[1803]

888. RISKS – The risks of cloud computing mirror its benefits. By externalising portions of IT infrastructure, the customer invariably gives up a certain degree of control.[1804] Servers, data and applications are no longer kept within the organisation,

---

[1797] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 14

[1798] W.K. Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary University of London, School of Law Legal Studies Research Paper No. 77/2011, 2011, p. 6, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130 (last accessed 18 December 2015) and L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1. A cloud provider typically manages a pool of hardware resources for resource efficiency: during periods of reduced consumer demand, the cloud provider may power off unused components. (L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 4-1).

[1799] J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *Revue du Droit des Technologies de l'Information* 2011, n° 42, p. 36 and B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *Revue de Droit Commercial* 2011, Vol. 10, p. 1001. Strictly speaking, cloud computing services can also be implemented on-site, on the customer's preferences (see L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.,* p. 4-4). The remainder of this chapter will approach the topic of cloud computing with the assumption that the cloud is hosted and operated in an offsite location (i.e., outside the organisation of the customer).

[1800] European Commission, "Unleashing the Potential of Cloud Computing in Europe", Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 529 final, 27 September 2012, p. 4.

[1801] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1.

[1802] European Commission, "Unleashing the Potential of Cloud Computing in Europe", *l.c.*, p. 2. It should be noted, however, that the term cloud computing is used in reference to a variety of systems and technologies and business models. Claims about the benefits of cloud computing are in fact only true for some kinds of cloud systems. For a more detailed discussion see L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 4-1 et seq.

[1803] European Commission, "Unleashing the Potential of Cloud Computing in Europe", *l.c.*, p. 4. This statement mainly holds true in case of public clouds, which are offered to the public at large. See L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, o.c., p. 8-4.

[1804] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 5-6.

but on the premises of one or more external providers.[1805] As a result, customers are by definition dependent on the cloud provider to implement appropriate measures to ensure the confidentiality and security of processing.[1806] Cloud customers may also lack sufficient information regarding the processing operations that take place.[1807] For example, cloud computing is typically associated with a sense of geographic indeterminacy:

> "*the use of hardware is dynamically optimised across a network of computers, so that the exact location of data or processes, as well as the information which piece of hardware is actually serving a particular user at a given moment, does not in principle have to concern the user, even though it may have an important bearing on the applicable legal environment.*"[1808]

From a business perspective, migrating to the cloud increases the customer's dependency on the availability and continuity of external services.[1809] Moreover, if the cloud provider uses proprietary technology, it may prove difficult for customers to shift data and documents between different cloud-based systems, which could lead to vendor lock-in.[1810]

889. OLD WINE, NEW BUSINESS MODEL? – Cloud computing is simply one of the latest evolutionary steps in the delivery of IT.[1811] In a sense, there is really "nothing new" about cloud computing. As noted by Marchini:

> "*the idea of obtaining use of a software application remotely is as old as computing; early software use involved access to mainframes with distributed dumb terminals or to data processing power through bureau services.*"[1812]

[1805] B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1001. It should be noted that there also exist on-site cloud solutions, in which case the cloud infrastructure is hosted on the customer's premises. For more information see L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 4-4.
[1806] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 5.
[1807] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 5.
[1808] European Commission, "Unleashing the Potential of Cloud Computing in Europe", *l.c.*, p. 3. See also L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1 and P. Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU", in N. Pohlmann, H. Reimer and W. Schneider (eds.), *ISSE 2010 Securing Electronic Business Processes*, Springer, 2010, p. 164-165. One might argue that the very metaphor of "cloud" computing, in fact, encourages a vision of something elusive, beyond control or regulation. See also T. McMullan, "How we talk about the cloud shapes the way we perceive internet privacy", *The Guardian*, 7 October 2015, available at http://www.theguardian.com/technology/2015/oct/07/the-cloud-internet-privacy-data-servers (last accessed 17 December 2015) ("*As a name, the cloud is at once a fluffy, approachable means to digest a global network of servers. It is also a vague, formless entity that grows and shrinks above our heads. In terms of privacy, it represents an important change in how we think about our data; stored in the arms of an invisible force, at once everywhere and nowhere.*").
[1809] P. Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU", *l.c.*, p. 165-166.
[1810] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 5. See also D. Svantesson and R. Clarke, "Privacy and consumer risks in cloud computing", *Computer Law & Security Review* 2010, Vol. 26, p. 391 et seq.
[1811] A. Joint and E. Baker, "Knowing the past to understand the present – issues in the contracting for cloud based services", *Computer Law & Security Review* 2011, Vol. 27, p. 408.

The main distinction, Marchini continues, is a distinction of scale: it has simply become more prevalent.[1813] Once again, a wide range of processing operations is taking place outside the walls of the organisation itself, in principle leaving the organisation with more time to focus on its own core activities.[1814] Another major difference concerns the technical foundation and organisation of cloud computing services, which cause data and data processing to be distributed dynamically among data centres located around to world.[1815]

890. TYPES OF CLOUD SERVICES – Cloud services are typically divided into three categories, depending on which IT resource forms the main object of the service (software, platforms, or infrastructure):[1816]

- *Software as a Service (SaaS)*: customers are able to remotely use the software applications offered by the provider, running on a cloud infrastructure;
- *Platform as a Service (PaaS)*: customers are able to deploy onto a cloud infrastructure (which acts as a "platform") consumer-created or -acquired applications (as long as they use the programming languages and tools supported by the provider);
- *Infrastructure as a Service (IaaS)*: customers are able to use processing, storage, networks, and other fundamental computing resources offered by the provider, whereby the consumer is free to deploy and run arbitrary software (which can include both operating systems and applications).

891. A SPECTRUM OF CONTROL – The three service models described above can be seen as a "spectrum" or "continuum", which ranges from low-level functionality (IaaS) to high-level functionality (SaaS), with PaaS in the middle.[1817] One could argue that the

---

[1812] R. Marchini, *Cloud computing: A Practical Introduction to the Legal Issues*, *BSI Standards Institution*, London, 2010, p. 2.
[1813] Id.
[1814] P. Schwartz, "Information Privacy in the Cloud", *University of Pennsylvania Law Review* 2013, Vol. 161, p. 1649. See also B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1003.
[1815] International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum", adopted 23-24 April 2012, p. 6.
[1816] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1/2. See also Leenes R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 3; D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 15; D. Bigo a.o., "Fighting cyber crime and protecting privacy in the cloud", *l.c.*, p. 13; B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1001; and Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 26. Another frequent classification is based on the *target user* of the service offered, which distinguishes between public, private, community or hybrid clouds. See e.g. S.Y. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *l.c.*, p. 663.
[1817] W.K. Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 6. See also S.Y. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *l.c.*, p. 663.

higher the functionality, the greater the control exercised by the cloud provider.[1818] In case of IaaS, the customer is essentially renting storage and processing capabilities, retaining full freedom to deploy whichever applications he sees fit. In case of SaaS, the functionality offered by the technology is defined completely by the provider. All the customer is expected to do is to access and consume the final product, no assembly required.

892. LAYERS OF CLOUDS – It should be noted that there may be layers of cloud providers involved in providing a service, sometimes without the customer's knowledge.[1819] For example, a SaaS provider might rely on an external IaaS and/or PaaS provider when offering its services to customers.[1820] In addition, both cloud providers and cloud customers can also combine cloud services from different cloud providers.[1821] For example, the customer of a PaaS provider might consume the services of multiple SaaS providers, whereas the PaaS provider itself might be a customer of multiple IaaS providers.

893. OUTLINE – The objective of this chapter is to analyse how the current data protection framework relates to the context of cloud computing. To this end, it will begin by describing the various actors involved in cloud computing and the interactions between them. Next, it will analyse the legal status ("role") of each actor, as interpreted by regulators and scholars. After that, it will describe the main responsibilities assigned to each actor, in particular by the Article 29 Working Party and national regulatory authorities. Once this analysis has been completed, this chapter will critically evaluate the relationship between the current framing of roles and responsibilities and the context of cloud computing.

894. SCOPE – For purposes of conceptual clarity, the remainder of this chapter limits itself to the discussion of public, offsite cloud services which involve the processing of personal data.[1822]

[1818] S.Y. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *l.c.*, p. 663.

[1819] W.K. Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 6,

[1820] *Id.* See also B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1002. ("*caractéristique marquante du cloud computing est la multiplicité et, subséquemment, l'opacité relative des acteurs auxquelles l'utilisateur peut se trouver confronté: ainsi, un service de stockage de documents ou de photos qui développe sa propre application et la commercialise en mode software as a service peut utiliser l'infrastructure d'un autre fournisseur (infrastructure as a service ou platform as a service*").

[1821] W.K. Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 6,

[1822] In other words onsite, private or community cloud services are outside the scope of the present analysis.

2 ACTORS

895. SELECTION CRITERIA – The current inventory of actors is based on a literature study of academic publications and regulatory guidance concerning privacy and cloud computing. A common denominator among the selected entities is that they each process personal data resulting in the context of cloud computing services.

896. ACTORS OVERVIEW – The following types of entities[1823] may be considered as the main entities involved in the operation of cloud computing services:

(1) Cloud customer, including end-users.

(2) Cloud providers, including

(a) Application providers;

(b) Platform providers; and

(c) Infrastructure providers.

897. VISUAL REPRESENTATION – The aforementioned entities interact with each other in a variety of ways. The following figure provides a – highly simplified – representation of how these entities might interact in the provisioning of cloud computing services. It is intended to be conceptual rather than factual.

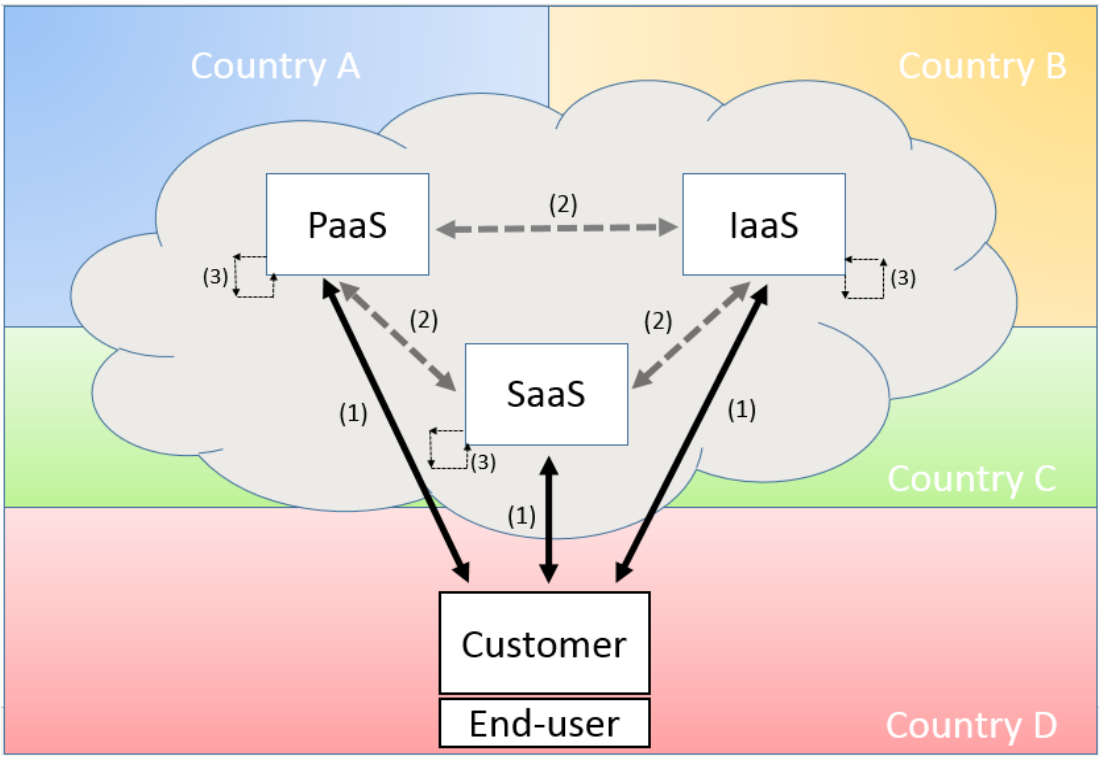

Figure 5 – Main entities involved in cloud computing

[1823] The term "entity" (instead of "actor") is used to signal that each identified "actor" could in principle be either a separate legal entity or a purely technical component operated.

898. LEGEND – The arrows in Figure 5 indicate that an exchange of personal data is taking place. Exchanges of personal data in the context of cloud computing are in principle bi-directional, as data is in principle disclosed with a view of further processing by the entity who disclosed it. Solid black arrows were used to depict data exchanges which may be actively initiated by the customer, depending on the service model (SaaS, PaaS or IaaS). Dashed grey arrows signify data exchanges which might be less obvious to cloud customers, depending on the service model and information provided by the cloud provider. The coloured segments were added to signal that that each entity might be located in a different jurisdiction. Over the following sections, a brief description is provided of each of the actors and interactions displayed in Figure 5.

899. COMBINATIONS POSSIBLE – The reader should note that the categories of actors identified in Figure 5 are not mutually exclusive. A given actor may combine multiple roles depending on the circumstances (e.g., a SaaS provider might also operate PaaS and/or IaaS services).

2.1 CLOUD CUSTOMER AND END-USER

900. MAIN CHARACTERISTICS – The cloud customer is the subscriber of a cloud computing service. It may be either a natural or legal person, or a group of natural and/or legal persons. Typical cloud customers include companies and self-employed businessmen who use cloud services in the exercise of their commercial activities (e.g., for purposes of customer relations management), as well as private individuals who use cloud services in a purely private capacity (e.g., to back-up personal photos).[1824] The end-user is the natural person who actually uses the cloud computing service in a specific context.[1825] The end-user may coincide with the cloud customer, but may also be a separate entity (e.g., an employee within the organisation of the cloud customer).[1826] Finally, it is worth noting that cloud customers may combine cloud services from different cloud providers.[1827]

901. DATA DISCLOSURE – Cloud customers and end-users access cloud services under a client-server model, which means that they send messages over a network to server computers, which then perform work in response to the messages received.[1828] The data disclosed to the service provider typically includes "first-party data" (e.g., data relating to the cloud customer or his employees) as well as "third-party data" (e.g. data relating to the clients of the cloud customer).

[1824] See also J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 36.
[1825] R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 3
[1826] Id.
[1827] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 6.
[1828] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 4-1.

902. DATA FLOWS – The interaction between cloud customers and cloud providers is depicted in figure 5 by way of arrows (1). The customer may be in direct communication with all three types of cloud providers, or only with a subset of them, depending on service model. In the latter case, the contracted cloud provider may enlist one or more other cloud providers to obtain the auxiliary services necessary to provide the functionality requested by the customer (arrows (2)).

2.2 CLOUD PROVIDER

A. Application provider (SaaS)

903. MAIN CHARACTERISTICS – Cloud application providers (SaaS) provide their customers with (1) the ability to use specific software applications on demand and (2) application data management services (e.g., backup and data sharing between consumers).[1829] The software applications offered by SaaS providers are often meant to replace conventional applications to be installed by users on their local systems.[1830] Commonly cited examples of SaaS services include: Microsoft's Office 365 (which includes office applications such as Word, Excel, PowerPoint, OneNote, Outlook, etc.)[1831], Salesforce.com (which includes customer relations management applications such as Sales, Marketing and Analytics)[1832], Google Docs (a collaborative word processing application), and Dropbox (a storage and sharing application).[1833]

904. DATA COLLECTION – Cloud application providers may collect various types of personal data. Salesforce.com, for example, distinguishes between the following types of data in its privacy notice[1834]:

1. *Contact information* (e.g., such as name, company name, address, phone number, and email address);
2. *Billing information* (e.g., billing name and address, credit card number, and the number of employees within the organisation that will be using the Services);

[1829] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 5-1.
[1830] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 26.
[1831] See Microsoft, "Office 365 for business FAQ", accessible at https://products.office.com/en-us/business/microsoft-office-365-frequently-asked-questions (last accessed 3 May 2016).
[1832] See Salesforce.com, "Products overview", accessible at http://www.salesforce.com/eu/products (last accessed 3 May 2016).
[1833] See R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 3, P. Schwartz, "Information Privacy in the Cloud", *l.c.*, p. 1633. Several authors also consider Facebook as an example of a SaaS application (see e.g. R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 3). Contra: D. Bigo a.o., "Fighting cyber crime and protecting privacy in the cloud", *l.c.*, p. 15.
[1834] Salesforce.com, *Privacy Statement*, 1 October 2014, available at http://www.salesforce.com/company/privacy/full_privacy.jsp (last accessed 21 December 2015).

3. *Optional information* (e.g., company annual revenues, number of employees, or industry);
4. *Web site navigational information* (e.g., Cookies, Web Beacons and IP Addresses);
5. *Submitted data* (e.g., data submitted to public forums, as part of a friend referral or as part of a testimonials);
6. *(Third-party) Customer data*: data submitted by Salesforce.com customers for storage and processing purposes (e.g., contact information of current and recurring customers, accounts, emails, calendars, and tasks)[1835]; and
7. *Data collected through mobile applications* (e.g., call records, pictures, geographic location, contact information).

905. DATA USAGE – Cloud application providers use the data collected from their customers and end-users in a variety of ways. Here too, a distinction should be made between "first-party data" and "third-party data". For example, Salesforce.com uses data about its customers and end-users ("first-party data") to communicate with its customers, enforce access privileges, market new products and improve its sites and services. Data submitted by Salesforce.com customers concerning their clients ("third-party data") are processed mainly for the purposes of providing the services requested by customers.[1836] Services offered by Salesforce.com, for example, include customer relations management ("Sales"), customer service ("Service"), marketing (including the use of predictive intelligence[1837] and management of advertising channels[1838]) and analytics services.[1839] It is not excluded, however, that cloud application providers also process data submitted by customers for purposes beyond the services requested.

906. DATA FLOWS – Arrow (1) depicts the flow of data between cloud application providers and their customers. As indicated earlier, there may be layers of cloud providers involved in providing a service. Arrow (2) signals the potential interaction between cloud application providers and cloud platform and/or cloud infrastructure

---

[1835] See e.g., Salesforce APAC, "Salesforce CRM Demo for Small Business", accessible at https://www.youtube.com/watch?v=mbo8_VHaBWw (last accessed 3 May 2016). Not all data is necessarily stored on Salesforce servers, may also just be indexed and referenced by Salesforce but stored locally.

[1836] According to the its privacy policy, Salesforce.com "*salesforce.com may access Customer Data only for the purposes of providing the services, preventing or addressing service or technical problems, at a Customer's request in connection with customer support matters, or as may be required by law*."

[1837] Salesforce.com, "Personalisation builder", accessible at http://www.salesforce.com/marketing-cloud/features/predictive-internet-intelligence (last accessed 3 May 2016).

[1838] L. Doyle, "Salesforce Marketing Cloud Brings Complete CRM to Digital Advertising Channels", Salesforce blog, 23 June 2015, available at https://www.salesforce.com/blog/2015/06/salesforce-marketing-cloud-brings-complete-crm-digital-advertising-channels.html.

[1839] For more information see Salesforce.com, "Products overview", accessible at http://www.salesforce.com/eu/products (last accessed 3 May 2016).

providers. Arrow (3) intends to illustrate that cloud customers may combine the services of multiple cloud application providers.

B. Platform provider (PaaS)

907. MAIN CHARACTERISTICS – Cloud platform providers (PaaS) provide their customers with tools and execution resources to develop, test, deploy and administer applications.[1840] Typical features include software development tools (e.g., programming languages, run-time environments), configuration management, and deployment platforms.[1841] PaaS services are usually addressed to market players that use them to develop and host applications either to meet in-house requirements or to deploy them as services to third parties.[1842] Commonly cited examples are Microsoft's "Azure"[1843], Salesforce.com's "Force"[1844] and Google's "App engine"[1845].[1846]

908. DATA COLLECTION – Cloud platform providers may collect various types of personal data. Microsoft, for example, distinguishes between the following types of data in relation to its Azure service[1847]:

1. *Customer data*: all data that are provided to Microsoft through use of the Online Service but excluding Administrator Data, Payment Data, or Support Data (e.g., text, sound, image or video files);
2. *Administrator data*: information provided to Microsoft during sign-up, purchase, or administration of the Online Services (e.g., name, address, phone number, and email address, as well as aggregated usage information and account controls);

[1840] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 6-1.

[1841] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 15 and L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 6-1.

[1842] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 26

[1843] See Microsoft, "Microsoft Azure", accessible at https://azure.microsoft.com/en-us (last accessed 3 May 2016).

[1844] See Salesforce.com, "Products overview", accessible at http://www.salesforce.com/eu/products. See also Certifiedondemand.com, "What is Salesforce.com?" available at https://www.youtube.com/watch?v=ToHiNvBON5A at 2:44 et seq. (last accessed 3 May 2016).

[1845] See Google Cloud Platform, "Google App Engine Documentation", accessible at https://cloud.google.com/appengine/docs (last accessed 3 May 2016).

[1846] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 15 and P. Schwartz, "Information Privacy in the Cloud", *l.c.*, p. 1633.

[1847] See Microsoft Azure, "Microsoft Azure Legal Information", April 2015, accessible at https://azure.microsoft.com/en-gb/support/legal; Microsoft, "Microsoft Online Services Privacy Statement", June 215, accessible at https://www.microsoft.com/privacystatement/en-us/OnlineServices/Default.aspx and Microsoft, "Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance", April 2015, p. 14, available at https://www.microsoft.com/en-us/Openness/TrustedCloud (last accessed 3 May 2014).

3. *Access control data*: data that is used to manage access to other types of data or functions within Azure (e.g., passwords, security certificates, and other authentication-related data);
4. *Metadata*: data concerning configuration and technical settings (e.g., disk configuration settings for an Azure virtual machine);
5. *Payment data* (e.g., credit card number, name and billing address, security code associated with the payment instrument, organisational tax ID);
6. *Support data* (e.g., information submitted in a support request form, chat sessions, information about hardware or software used, error-tracking files);
7. *Cookies & similar technologies* (e.g., web beacons, analytics cookies); and
8. *Data collected through local software* (e.g., data about the use or performance of software agents or device management applications installed on a device).

909. DATA USE – Cloud platform providers use the data collected from their customers and end-users in a variety of ways. Once again, a distinction should be made between "first-party data" and "third-party data". For example, Microsoft uses data about its Azure customers and end-users ("first-party data") to communicate with its customers, to complete transactions and to ensure quality of service. Data submitted by Azure customers, which may concern individuals other than the customer or end-users ("third-party data") shall in principle only be processed for the purposes of providing the Azure services as requested by customers.[1848] Azure platform services include, for example, app development and testing, API management and application insights.[1849] Finally, it should be noted that while Azure was conceived of as a cloud platform service (PaaS), it also enables customers to host external, already existing applications (IaaS) and to run software written by Microsoft itself (SaaS) (e.g., analytics).[1850]

910. DATA FLOWS – Arrow (1) depicts the flow of data between cloud platform providers and their customers. Arrow (2) signals the potential interaction between cloud platform providers and cloud application and/or cloud infrastructure providers. Arrow (3) intends to illustrate that cloud customers may combine the services of multiple cloud platform providers.

[1848] Microsoft, "Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance", *l.c.*, p. 14 ("*Microsoft will not use customer data or derive information from it for advertising. We will use customer data only to provide the service or for purposes compatible with providing the service*" ; Microsoft online services Privacy statement: "*Customer Data will be used only to provide customer the Online Services including purposes compatible with providing those services. For example, we may use Customer Data to provide a personalized experience, improve service reliability, combat spam or other malware, or improve features and functionality of the Online Services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes.*")

[1849] See Microsoft, "Microsoft Azure", accessible at https://azure.microsoft.com/en-us (last accessed 3 May 2016).

[1850] See A. Chauhan, V. Fontama, M. Har a.o., "Introducing Microsoft Azure HDInsight Technical Overview", Microsoft Press, 2014, p. 24.

C. *Infrastructure provider (IaaS)*

911. MAIN CHARACTERISTICS – Cloud infrastructure providers (IaaS) provide their customers with access to virtual computers, storage, infrastructure components and configuration services.[1851] Customers typically rely on IaaS to replace corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems.[1852] Hardware resources are typically allocated to customers in the form of "virtual machines" (or "instances") which they can consume on demand ("dynamic resource renting").[1853] Customers are in principle able to install the operating system(s) and applications of their choosing.[1854] Commonly cited examples of IaaS include Amazon's Elastic Compute Cloud (EC2)[1855] and Simple Storage Service (S3)[1856] and Rackspace Cloud[1857].[1858]

912. DATA COLLECTION – Cloud infrastructure providers may collect various types of personal data. Amazon, for example, distinguishes between the two types of data: account information and customer content. Account information concerns information that E2C customers provide to Amazon in connection with the creation or administration of their Amazon Web Services (AWS) account (i.e. "first-party data").[1859] Customer content essentially refers to data stored by end-users on Amazon systems when using AWS[1860], which may (but does not necessarily) include personal data relating to third parties (i.e. "third-party data").[1861]

[1851] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-1.

[1852] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 26

[1853] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-1/3. For a description of "virtualisatoin" see L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-2; W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 17 and S. Marston a.o., "Cloud computing — The business perspective", *Decision Support Systems* 2011, Vol. 51, p. 178.

[1854] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-2.

[1855] Amazon Web Services, "Amazon EC2 - Virtual Server Hosting", accessible at https://aws.amazon.com/ec2 (last accessed 3 May 2016).

[1856] Amazon Web Services, "Amazon S3", accessible at https://aws.amazon.com/s3 (last accessed 3 May 2016).

[1857] See http://www.rackspace.co.uk.

[1858] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 15. See also S. Marston a.o., "Cloud computing – The business perspective", *Decision Support Systems* 2011, Vol. 51, p. 178.

[1859] Use of Amazon's E2C service is covered by the Amazon Web Services (AWS) privacy policy which apply to all Amazon web services generally. See Amazon Web Services, "AWS Privacy", accessible at https://aws.amazon.com/privacy (last accessed 3 May 2016). Data collected by Amazon in relation to its customers include provided information (e.g. basic account information, information provided in a form or through a review), information sent as part of internet communication (e.g. IP address, browser information), purchase history, cookies, device information, information from other sources, …

[1860] Amazon Web Services, "AWS Privacy", accessible at https://aws.amazon.com/privacy (last accessed 3 May 2016).

[1861] Amazon formally defines "customer content" as "*customer content as software (including machine images), data, text, audio, video or images that a customer or any end user transfers to us for processing,*

913. DATA USE – The Amazon AWS privacy policy outlines the following forms of data use:

1. Completing transactions (processing payments, fulfilling orders);
2. Customer communication (e.g. promotional offers);
3. Analytics;
4. Advertising (including advertising on third-party websites); and
5. Customer service.

The Amazon AWS privacy policy in principle only applies to customer's account information and not to content stored by customers on Amazon systems.[1862] Amazon states it does not access or use customer content "*for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users*".[1863]

914. DATA FLOWS – Arrow (1) depicts the flow of data between cloud infrastructure providers and their customers. Arrow (2) signals the potential interaction between cloud infrastructure providers and cloud platform providers and/or cloud software providers. Arrow (3) intends to illustrate that cloud customers may combine the services of multiple cloud infrastructure providers.

---

storage or hosting by AWS services in connection with that customer's account and any computational results that a customer or any end user derives from the foregoing through their use of AWS services." http://aws.amazon.com/compliance/data-privacy-faq/

[1862] Amazon Web Services, "AWS Privacy", accessible at https://aws.amazon.com/privacy (last accessed 3 May 2016).

[1863] Amazon Web Services, "Data Privacy", accessible at http://aws.amazon.com/compliance/data-privacy-faq (last accessed 3 May 2016).

3 ROLES

3.1 CLOUD CUSTOMERS AND END-USERS

915. HIGH-LEVEL ANALYSIS – Cloud customers are generally viewed as "controllers" in relation to the processing of (third-party) personal data they entrust to cloud providers.[1864] Cloud customers determine both the "purposes" and "means" of the processing, in that they decide

(1) for which purposes to use cloud services (e.g. in furtherance of their commercial or other objectives);

(2) which cloud services to use and, by extension, how personal data shall be processed; and

(3) which cloud provider to enlist.

To the extent that the end-user and cloud customer coincides, he or she will be considered the controller of the processing. Employees who process personal data on behalf of the cloud customer are "persons acting under the authority of the controller" within the meaning of article 16 of Directive 95/46.[1865]

It is also possible that a cloud customer contracts a cloud service in order to process personal data on behalf of a third party (who may actually be the controller or simply another entity in the supply chain).[1866] In such cases, it is possible that the cloud customer acts only as a processor.[1867]

916. SCOPE OF CONTROL – In practice, the control exercised by the cloud customer regarding the means of the processing may be limited. More often than not, cloud services are offered under standard terms, on a "take it or leave it basis".[1868] Depending

---

[1864] See e.g. J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *Computerrecht* 2011, Afl. 3, p. 110; B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1009; A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *European Journal for Law and Technology* 2012, Vol. 3, No. 2, available at http://ejlt.org/article/view/96/253; Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 8; Information Commissioner's Office (ICO), "Guidance on the use of cloud computing", *l.c.*, p. 7; Commission Nationale de l'Informatique et Libertés (CNIL), "Recommendations for companies planning to use Cloud computing services", 25 June 2012, p. 5, available at http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf (last accessed 2 January 2016).

[1865] Cf. *supra*; nrs. 151 et seq.

[1866] Amazon Web Services, "Whitepaper on EU Data Protection", October 2015, p. 10, available at http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf (last accessed 2 January 2016).

[1867] See also *infra*; nr. 950 and *supra*; nr. 183 et seq. for a discussion of the requirements in case of sub-processing.

[1868] See also L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 3-1.

on the nature of the cloud service (SaaS, PaaS or IaaS), the cloud customer will be able to exercise greater or less control over the manner in which the processing is operated:[1869]

- *SaaS*

In case of SaaS, the cloud customer essentially only has control over the application-specific resources which the SaaS application makes available.[1870] The processing capabilities of the cloud customer are dependent and the features and services supported by the software offered by the cloud provider. For example, if the cloud provider offers an email application, the customer will typically have the ability to create, edit or send messages.[1871] Depending on the service, the customer may also enjoy limited administrative control over the application. For example, in the case of the email application, the cloud customer may have the ability to create new accounts for end-users and/or review the activities of end-users.[1872] It should be noted, however, that the processing capabilities (and thus also the scope of control of cloud customers) may vary widely across SaaS applications (compare e.g., Salesforce.com with Dropbox services).

- *PaaS*

In case of PaaS, the cloud customer in principle has complete control over which applications shall be implemented and deployed (as long as he uses the programming languages and tools supported by the provider).[1873] The customer is granted access to programming and utility interfaces, which provide him with an execution environment to run his applications and access to the necessary computing resources (e.g., memory, persistent storage, data stores, data bases and network connections).[1874] The cloud customer in principle enjoys complete administrative control over the applications deployed, which may be either consumer-created or acquired. It should be noted, however, that the provider of the PaaS service may offer its customers to run applications written by the provider (in which case this portion of the service corresponds to a SaaS model) or to host external, already existing applications (in which case this portion of the service corresponds to an IaaS model).[1875]

- *IaaS*

In case of IaaS, the cloud customer enjoys complete control over the computing resources offered by the provider, which are typically presented in the form of "virtual machines" (VMs). The customer has full control over the operation of the guest

[1869] See also *infra*; nrs. 923 et seq.
[1870] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 5-3.
[1871] *Id.*
[1872] *Id.*
[1873] *Ibid*, p. 6-3.
[1874] *Id.*
[1875] See also *supra*; nr. 909.

operating system in each VM and is free to deploy and run arbitrary software.[1876] Under the IaaS service model, the customers typically carries the burden of operating, updating and configuring the rented computer resources for security and reliability.[1877] It should be noted, however, that the provider of an IaaS service may also offer its customers applications written by the provider (in which case this portion of the service corresponds to a SaaS model) or to host external, already existing applications (in which case this portion of the service corresponds to an IaaS model).

The amount of control which cloud customers enjoy in determining the "means" of the processing thus varies significantly across service models. In case of SaaS, the ability for the customer to influence the means of the processing shall be very limited. In case of IaaS, the customer enjoys practically the same level of privileges as if the owned computing resources himself. Even in case of SaaS, however, the cloud customer still determines the means of the processing by choosing to process personal data through a particular cloud service.

917. PERSONAL USE EXEMPTION – Cloud computing services are consumed not only by businesses and governments, but also be individuals acting in the course of personal or household activity. The latter shall in principle be exempted from compliance in accordance with article 3(2) of Directive 95/46, unless the data is made available to an indefinite number of people.[1878]

3.2 CLOUD PROVIDER

918. PRELIMINARY DISTINCTION – Section 2 illustrated that cloud providers may provide a wide variety of services, each of which may involve the processing of personal data. While there is agreement among scholars and regulators as to the legal status of the cloud customer, the legal status of the cloud provider appears to be less clear-cut. At the outset, a distinction must be made between data about the customers themselves ("first party-data") and data submitted by customers to the cloud provider for further processing ("third-party data").[1879]

919. FIRST-PARTY DATA – Every cloud provider, regardless of service model, acts as a controller when processing personal data about its customers for purposes of account creation, administration and billing (first party-data). The same applies also in relation to data processing undertaken by the cloud provider to improve its services (e.g., use of site analytics to monitor performance) or to market new products. For those sets of

[1876] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-2.
[1877] *Id.* In case of PaaS and Saas, these aspects are typically taken care of by the cloud provider (*Id.*).
[1878] Cf. *supra*; nrs. 869 et seq.
[1879] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 11-12.

processing operations, the cloud provider clearly determines the purposes and means of the processing.

920. THIRD-PARTY DATA – As far as the processing of third-party data is concerned (i.e. data entrusted to the cloud provider for further processing), many scholars and regulators seem inclined to assign the cloud provider the role of processor.[1880] Others point out that there may be situations in which the cloud provider should be considered as a (joint) controller.[1881] Finally, certain scholars defend the viewpoint that there may be situations in which the cloud provider should be viewed as neither a controller nor processor.[1882] But almost all agree that the legal status of the cloud provider must be assessed in light of the actual services provided, the interactions between the parties and the set of data or operations at issue.[1883]

921. HETEROGENOUS CONCEPT – The divergent viewpoints regarding the legal status of the cloud provider may be explained, at least in part, because of heterogeneous nature of the concept of "cloud computing". The concept of cloud computing encompasses many different service models (SaaS, PaaS and IaaS), which each have different properties and foresee varying degrees of control for customers and providers respectively. Second, the concept is sometimes understood so broadly that it becomes difficult to conceive of any internet application which would not be considered a cloud service.[1884] Finally, there is a great variety among cloud computing services, even within a particular service model (compare e.g., Salesforce.com with Dropbox services).

[1880] A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *European Journal for Law and Technology* 2012, Vol. 3, No. 2, available at http://ejlt.org/article/view/96/253; D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 46, Determann, L., "Data Privacy in the Cloud—Myths and Facts", Institute for IT Law, 10 April 2012, online publication at http://www.iitr.us/publications/40-data-privacy-in-the-cloud-a-dozen-myths-and-facts.html, Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 7-8 (but there may be exceptions: Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 20); Information Commissioner's Office (ICO), *Guidance on the use of cloud computing*, *o.c.*, p. 7-10.

[1881] See e.g. R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 8; J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 110-111; De Hert, P., Papakonstantinou, V. and Kamara, I., "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection", *l.c.*, p. 17-18; F. Gilbert, "Cloud service providers as joint-data controllers", *Journal of Internet law* 2011, p. 3-12; European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe'", 16 November 2012, paragraphs 46-48 and Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 6.

[1882] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 14 et seq.

[1883] See e.g., B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1002 ; J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 110-111; P. Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU", *l.c.*, p. 168 and P. De Hert, V. Papakonstantinou and I. Kamara, "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection", *l.c.*, p. 18.

[1884] For example, several authors consider OSNs as an example of cloud computing. See e.g. R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 6.

922. OUTLINE - The main objective of this section is to provide an inventory of the arguments advanced by scholars and regulators regarding specific cloud service models in support of the view that the provider should be considered as either a controller, joint controller or processor. Given the heterogeneous nature of cloud services the analysis of the roles of cloud providers in the sections that follow should be reviewed with great caution. This section does not seek to provide a definitive qualification of the role of the providers of different types of cloud services. A case-by-case analysis remains indispensable. For purposes of conceptual clarity, the analysis shall be limited the processing of third-party data by cloud providers.

A. Application providers (SaaS)

923. RELEVANT CHARACTERISTICS – In case of SaaS, the cloud provider offers its customers the ability to consume software applications remotely. A typical SaaS provider manages the underlying cloud infrastructure (including network, servers, operating systems, storage), decides which applications to offer, and may also decide about individual application capabilities.[1885] The SaaS provider configures and manages the operation of the application so that it provides expected service levels to consumers.[1886] At a technical level, the SaaS provider retains ultimate authority over the application.[1887] While the customer may enjoy a certain level of administrative control, such control exists only at the discretion of the provider.[1888]

924. LEGAL STATUS – The legal status of SaaS providers appears to be the most ambiguous of all cloud service models. There are essentially three different ways in which this issue has been approached by scholars and regulators, each of which will be elaborated of the following paragraphs.

925. PROVIDER AS PROCESSOR – A first group of scholars and regulators seem predisposed to consider all cloud providers as processors.[1889] While acknowledging that there may be exceptions, these authors emphasize that (a) the initiative to use the cloud service lies with the cloud customer and (b) the customer has ability to choose which cloud service best suits its needs.[1890] Certain authors also point out that the cloud

---

[1885] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 2-1/2.
[1886] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 5-3.
[1887] *Id.*
[1888] *Id.*
[1889] Cf. *supra*; footnote 1880. It should be noted, however, that these scholars and regulators do not necessarily distinguish among cloud service models (SaaS, PaaS or IaaS) when assessing the legal status of cloud providers.
[1890] Information Commissioner's Office (ICO), *Guidance on the use of cloud computing*, *o.c.*, p. 7-9; Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 7-8; A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *l.c.*, section 3.1.

customer is usually the entity who collected information from data subject and therefore already subject to data protection law.[1891] Alessandro Mantelero additionally argues that the decision-making power of cloud providers is not sufficient to consider them autonomous data controllers.[1892] Finally, Lothar Determann argues that cloud providers tend to offer platforms and software "*without any interest, knowledge, or influence regarding data types and processing purposes*".[1893]

926. PROVIDER AS SEPARATE CONTROLLER – A second group of commentators view SaaS providers as controllers in their own right, but only with respect to the additional uses determined by the cloud provider.[1894] For example, the SaaS provider which authorizes itself use data entrusted by customers for purposes of marketing or delivery of value-added services, should be considered as controllers in respect of these processing operations.[1895] If the activities of the provider remain limited, however, to the "processing mandate" given by the cloud customer, the SaaS provider would be deemed a mere processor.[1896]

927. PROVIDER AS JOINT CONTROLLER – A third group argues that certain SaaS providers should be considered as joint controllers rather than processors.[1897] These authors emphasize that SaaS providers effectively determine the "means" of the processing, often on a unilateral basis. SaaS providers design, operate and maintain software services with specific uses in mind.[1898] They determine the features and processing capabilities of the services they offer and choose which tools to use, whereas customers can only decide about certain settings.[1899] As a result, SaaS customers may

---

[1891] A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *l.c.*, section 3.1.
[1892] *Id.*
[1893] L. Determann, "Data Privacy in the Cloud—Myths and Facts", *l.c.*, Myth 10.
[1894] B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1009 and J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 44-45.
[1895] B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1009. See also Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 8
[1896] *Id.*
[1897] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 12-14; Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 5-6; F. Gilbert, "Cloud service providers as joint-data controllers", l.c., p. 7-8; J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 110-111.
[1898] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 13; F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 10 *("[…] a SaaS model where the SaaS provider has developed an application for which it has determined the features and proposed uses, and the customer is only able to assert its control over the use of the data hosted by the SaaS by deciding some specific settings. In this case, it would seem likely that at least some SaaS offerings might qualify as "data controllers."*)
[1899] F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 10. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 12 ("*When looking at*

have little or no influence over how (or where) personal data are processed.[1900] Moreover, cloud services are offered through standard contracts, with little or no possibility to negotiate special terms.[1901] The customer may therefore be unable to give the cloud provider "instructions" as envisaged by article 17(3) of Directive 95/46.[1902] Similarly, the contract between the SaaS provider and its customers may not enable customers to monitor or audit the provider's practices (which in turn implies that the customer cannot verify compliance with security and confidentiality guarantees).[1903] Finally, it is also pointed out that SaaS providers typically enjoy much greater technical expertise than their customers.[1904]

B. Platform provider (PaaS)

928. RELEVANT CHARACTERISTICS – In case of PaaS, the cloud provider offers its customers the ability to develop, test, deploy and administer applications.[1905] PaaS providers manage the underlying cloud infrastructure (e.g., operating system, servers, networks) and determine the programming models that customers can use.[1906] PaaS

SaaS solutions like cloud-based office productivity tools or business intelligence tools, the cloud client usually has no possibility to influence the type of service offered by the provider. In addition, the relationship between provider and client may not involve any direct negotiation and may amount to a simple registration process. As a consequence, the level of control over the means of the processing operations by the cloud client may be extremely limited. In this scenario, the EDPS considers that the qualification of the cloud service provider as co-controller might be more appropriate.")

[1900] J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 110 and European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 13.

[1901] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 13 and Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 5.

[1902] In contrast, Mantelero argues that cloud providers are bound to act on the instructions of their customers by virtue of the contract between them (even if those instructions have taken the form of standard clauses drafted by the cloud provider). (A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *l.c.*, section 3.1.)

[1903] Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 6 and F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 9. Article 17(2) of Directive 95/46 requires controllers to ensure compliance with technical security measures and organisational measures governing the processing. Cf. *supra*; nr. 84.

[1904] F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 9 ("*The "expertise of the parties" test may also be crucial in the case of cloud services. Indeed, in many cases the customer uses the service because it does not have the expertise to run these functions in-house. This is especially the case for SaaS providers, and it is indeed one of the primary selling points used by these service providers. They provide the technical expertise to achieve a particular goal, for example the operation of a CRM system, so that the customer may focus on the important activities that are directly related to the unique expertise of the customer, such as the development, marketing, and sale of its own products and services. Would not a cloud service provider that flaunts its expertise at a particular task (such as the design and operation of a CRM database) be in a position similar to that of the accountant [as described in WP169]?*")

[1905] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 6-1.

[1906] *Ibid*, p. 6-3.

providers in principle have no role (administrative or otherwise) in relation to the applications which are developed or run over their infrastructure.[1907]

929. LEGAL STATUS – Compared to SaaS, the influence of the provider of a PaaS service is much more limited. Its sphere of influence is confined to the lower levels of the software stack (hardware, operating system), with the exception of the programming and utility interfaces which the provider makes available to customers.[1908] It is therefore not surprising that many authors would consider PaaS providers as processors rather than controllers.[1909] Nevertheless, at least one regulator has signalled that there may be instances in which PaaS providers might nevertheless be considered controllers.[1910]

930. PROVIDER AS PROCESSOR – Microsoft has positioned itself as a processor in relation to its PaaS service "Azure" as well as other Microsoft cloud services. In April 2014, the Article 29 Working Party acknowledged that Microsoft's data processing agreement is in line with Commission Decision 2010/87/EU (standard contractual clauses for transfers to processors).[1911] Strictly speaking, the finding of conformity between Microsoft's contracts and the EU model clauses does not confirm Microsoft's status as processor. It does confirm, however, that at least from a contractual perspective the relationship between Microsoft and its Azure customers is consistent with a controller-processor relationship. In addition, it is also worth noting that the British Standards Institution (BSI) has validated that Azure is compliant with the ISO/IEC 27018 code of practice for the protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.[1912]

931. PROVIDER AS JOINT CONTROLLER – In its 2012 guidance, the CNIL noted that certain PaaS providers may be considered as joint controllers. Specifically, it reasoned that in some cases of public PaaS, customers have no real power to give the provider instructions and are not in a position to monitor the effectiveness of the security and

---

[1907] *Id.* As indicated earlier, it is possible that that the provider of the PaaS service may offer its customers to run applications written by the provider (in which case this portion of the service corresponds to a SaaS model) or to host external, already existing applications (in which case this portion of the service corresponds to an IaaS model). Cf. *supra*; nr. 916.

[1908] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 6-3.

[1909] See e.g. L. Determann, "Data Privacy in the Cloud—Myths and Facts", *l.c.*, Myth 10.

[1910] Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 5-6.

[1911] Article 29 Data Protection Working Party, Email to Ms Dorothee Belz, 2 April 2014, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf The finding also in relation to other Microsoft cloud services, including SaaS service Office 365. See also B. Smith, "Privacy authorities across Europe approve Microsoft's cloud commitments", *Official Microsoft Blog*, 10 April 2014, accessible at http://blogs.microsoft.com/blog/2014/04/10/privacy-authorities-across-europe-approve-microsofts-cloud-commitments (last accessed 3 May 2016).

[1912] See L. Woehler, "Microsoft Azure: The first cloud computing platform to conform to ISO/IEC 27018, the only international set of privacy controls in the cloud", *Microsoft Azure Blog*, 16 February 2015, accessible at https://azure.microsoft.com/en-us/blog/azure-first-cloud-computing-platform-to-conform-to-isoiec-27018-only-international-set-of-privacy-controls-in-the-cloud/ (last accessed 3 May 2016).

confidentiality guarantees given by the cloud provider.[1913] The CNIL considered that in such circumstances it may be appropriate to consider the cloud provider as joint controller.[1914]

C. Infrastructure provider (IaaS)

932. RELEVANT CHARACTERISTICS – In case of IaaS, the cloud provider provides its customers with access to virtual computers.[1915] The IaaS provider uses a Virtual Machine Monitor (VMM) or "hypervisor" to synthesize one or more virtual machines from its pool of hardware resources.[1916] The cloud provider manages only the underlying cloud infrastructure (hardware, networks) and hypervisor.[1917] A typical IaaS provider has no role (administrative or otherwise) in relation to either the applications or operating systems which are run over its infrastructure.[1918]

933. LEGAL STATUS – The provider of an IaaS services in principle has no control over the processing activities that take place on its virtual machines. The IaaS customer typically enjoys complete control over its virtual machine, the guest operating system and all software application layers above it.[1919] IaaS providers can nevertheless process (store, copy, delete) personal data "on behalf" of their customers. Many authors would therefore consider IaaS providers as "processors". Certain authors argue, however, that the provider of an IaaS service should not even be considered a processor.[1920]

934. PROVIDER AS PROCESSOR – Amazon has positioned itself as a processor in relation to its Elastic Compute Cloud (EC2) and other Amazon Web Services (AWS).[1921] AWS offers its customers a "data processing addendum" which, similar to Microsoft's data processing agreement, is considered to be in line with Commission Decision

---

[1913] Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 5-6.

[1914] *Ibid*, p. 6. Van der wees likewise indicates that there may be situations in which the PaaS provider acts as a (joint) controller, but its actual legal status should be determined in light of the services being offered and underlying contractual arrangements. (J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 111).

[1915] L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 7-1.

[1916] *Id.*

[1917] *Id.*

[1918] *Id.* Again, it should be noted that the provider of an IaaS service may also offer its customers applications written by the provider (in which case this portion of the service corresponds to a SaaS model) or offers a programming environment that enable customers develop and run new applications (in which case this portion of the service corresponds to an PaaS model). In such situations, the analysis regarding SaaS and PaaS providers applies rather than the analysis concerning IaaS.

[1919] *Id.*

[1920] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 14 et seq.

[1921] For more information see Amazon Web Services, "EU Data Protection", accessible at https://aws.amazon.com/compliance/eu-data-protection (last accessed 3 May 2016).

2010/87/EU (standard contractual clauses for transfers to processors).[1922] AWS has also been validated for compliance with ISO 27018.[1923] AWS's data processing addendum explicitly states that Amazon Web Services acts as a processor or sub-processor in relation to customer data (i.e. any personal data that is uploaded to AWS under the customer's AWS account).[1924]

935. "NOT EVEN A PROCESSOR" – Kuan Hon and others have argued that there are several instances in which the provider of a cloud service should not be considered as processors, but rather as neutral intermediaries within the meaning of the E-Commerce Directive.[1925] These authors point out that many cloud providers, especially infrastructure providers, may not have any knowledge or awareness of the fact that their systems are used to process personal data.[1926] They also argue that there are situations where the cloud provider may not even be able to determine whether the data processed using its infrastructure is personal in nature (e.g., in case of encrypted or anonymised data).[1927] Moreover, they consider that it is the customer who actually "processes" the data, whereas the cloud provider merely provides the technical infrastructure to do so.[1928]

[1922] See Commission Nationale pour la Protection des Données (Luxembourg), Letter to Mr. Dubois regarding the AWS data processing addendum, 6 March 2015, accessible at http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/AWS-3-6-15.pdf (last accessed 3 May 2016).

[1923] See Amazon Web Services, "Data Privacy", accessible at http://aws.amazon.com/compliance/data-privacy-faq (last accessed 3 May 2016).

[1924] Section 2.1 of Annex 1 of AWS' data processing addendum.

[1925] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 14 et seq.

[1926] *Ibid*, p. 18-19 and 27.

[1927] *Ibid*, p. 19 (""*[I]t is arguable that infrastructure providers are not even 'processors', particularly where they are used only for processing power. It is more difficult to do so where the service provided consists of or includes persistent storage of data, in other words where the provider acts as a data host. However, the provider will often not know the nature of data stored with it, so it seems problematic that its status should depend on what data its customer decides to store and how well the customer encrypts or anonymises the data.*").

[1928] *Ibid*, p. 16 and p. 19-20 ("*It should be borne in mind that when cloud services, whether IaaS, PaaS or SaaS, comprise 'pure' passive, infrastructure-like data storage facilities ('utility storage'), it is the user who chooses what kind of data to store on the provider's equipment, and in what form. The provider has no control over the user's actions here. Utility storage providers are unlikely to know whether the user is storing personal data or non-personal data, unless and until they inspect the data. This strengthens the argument that incidental access should not render these kinds of utility providers 'processors'.*")

4 ALLOCATION OF RESPONSIBILITY AND RISK

936. OUTLINE – In its Opinion on cloud computing, the Article 29 Working Party analysed the allocation of responsibilities between cloud customers and cloud providers from the perspective of a controller-processor relationship.[1929] The analysis in the sections that follow takes a similar point of departure. Where appropriate, however, reference shall also be made to situations in which the cloud provider acts as a joint controller. As was the case with the analysis of the role of the cloud provider (section 3.2), the analysis here shall be limited the processing of third-party data by cloud providers.

4.1 TRANSPARENCY

937. CLOUD CUSTOMER – As a controller, the cloud customer is obliged to ensure transparency of processing of data subjects. At a minimum, the data subject must be informed of the identity of the controller and the purposes of the processing. The Article 29 Working Party considers that cloud customers should "as a matter of good practice" inform data subjects about the identity of the cloud provider and all subcontractors (if any), as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors.[1930]

938. CLOUD PROVIDER – The cloud customer can only acquit its transparency obligations towards data subjects if it receives sufficient information from the cloud provider.[1931] According to the Article 29 Working Party, the cloud provider should therefore inform the customer of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres where personal data may be processed at.[1932] In cases where the cloud provider acts as a joint controller, the provider is also responsible for ensuring compliance. In such situations, the CNIL recommends that the information be provided by the entity to whom the data subjects have communicated their data.[1933]

[1929] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 4 ("*This opinion focuses on the situation, where the relationship is assumed to be a controller-processor relationship, with the customer qualifying as controller and the cloud provider qualifying as processor. In cases where the cloud provider acts as a controller as well, they have to meet additional requirements.*")

[1930] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 20. Such information shall be deemed mandatory in case where it is necessary to ensure fairness of processing. (*Ibid*, p. 10-11) See also J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 46.

[1931] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 11.

[1932] *Ibid*, p. 11. See also Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", WP 232, 22 September 2015, p. 6 and Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 8-9.

[1933] Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 6 ("*Although the customer and the service provider, both data*

939. ASSESSMENT – In its guidance, the Working Party seemingly leverages the customer's obligation to ensure transparency towards data subjects used to stimulate cloud providers – even those who act as processors – to be transparent towards their customers. While failure to provide such information may inhibit an organisation from using a particular cloud service, there is no direct obligation to provide such information under Directive 95/46 unless the cloud provider is deemed a controller. Even if the provider is deemed a controller, however, the cloud customer may in practice remain ultimately responsible for communicating the necessary information towards data subjects (as the customer is often the entity which has direct contact with the data subject).[1934]

4.2 DATA QUALITY

A. Purpose specification and use limitation

940. CLOUD CUSTOMER – The cloud customer is under an obligation to ensure that personal data are not processed for purposes which are incompatible with the purpose for which the data were collected.[1935] To this end, the cloud customer should obtain appropriate commitments from the cloud provider (including technical and organisational safeguards, such as access control, logging and auditing), which should in turn be captured in appropriate contractual safeguards.[1936]

941. CLOUD PROVIDER – In order to retain its status as processor, the cloud provider may not process personal data for any purpose not authorized by the controller. In particular, the cloud provider

> "*should configure its role as a mere leverage in the hands of the controller, with no involvement in the semantics of the processing and no margin of maneuver for any sort of further processing*".[1937]

942. ASSESSMENT – As with most controller-processor relationships, compliance with the purpose specification and use limitation principle requires contractual safeguards that limit the cloud provider's ability to process the data beyond purposes identified in

---

controllers, are responsible for the provision of information, in practice it is preferable that the entity to which the data subjects have communicated their data informs them of the processing means used by the service provider. Consequently, the service provider must give the customer all the information necessary to meet his obligation of provision of information. However, the service provider must remain the contact to whom the data subject must refer to obtain more information on the processing for which the service provider acts as joint controller.")

[1934] See also B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1014.

[1935] Article 6(1)b of Directive 95/46/EC.

[1936] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 11 and p. 20.

[1937] Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 9.

the contract between the cloud provider and customer. Any processing of personal data beyond the controller's instructions shall in principle render the cloud provider a controller.[1938]

B. Retention of data

943. CLOUD CUSTOMER – The cloud customer is under an obligation to ensure that personal data are not kept in identifiable form for longer than is necessary.[1939] Insecure or incomplete deletion of personal data is a real concern in cloud environments, as data may be kept redundantly on different servers at different locations.[1940] The cloud customer should therefore obtain adequate guarantees, in particular through contractual measures, that data shall be deleted securely by the cloud provider once the cloud customer has requested deletion.[1941]

944. CLOUD PROVIDER – The cloud customer is dependent on the cloud provider to implement deletion of data. According to the Article 29 Working Party, secure erasure of personal data requires that either the storage media are destroyed or demagnetized or the stored personal data are deleted effectively through overwriting.[1942] The cloud provider should therefore document its deletion practices and make available tools which allow the cloud customer to easily request deletion.

945. ASSESSMENT – Once again, the cloud customer is dependent on the cooperation of the cloud provider to ensure compliance with data protection requirements. Directive 95/46/EC does not impose upon the processor a direct obligation to comply with deletion requests emanating from the controller (it requires a contractual or other arrangement binding the processor to the controller's instructions). The continued storage of customer content after deletion has been requested by the cloud customer would, however, render the cloud provider a controller in relation to any further processing activities.

[1938] See also Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 8 ("*The CSP may cease to be considered a processor, with all its consequences especially in terms of liability, in cases where the actions taken by the CSP exceeds by far the normal capacities of a data processor in viewed of its supposed absence of autonomy with respect to the instructions of the controller*".)

[1939] Article 6(1)e of Directive 95/46.

[1940] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 12. See also D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 10 and 40.

[1941] *Id.* The CNIL additionally recommends including a clause in the contract between the cloud provider and customer which enable an of audit deletion logs either by the customer or by a trusted third party of the customer's choosing (Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 14).

[1942] *Id.*

4.3 CONFIDENTIALITY AND SECURITY

946. CLOUD CUSTOMER – As a controller, the cloud customer is responsible for ensuring the confidentiality and security of processing.[1943] The cloud customer must therefore (a) choose a cloud provider supplying sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out; and (b) must ensure compliance with those measures.[1944] In practice, this requires cloud customers to perform a comprehensive *risk assessment*.[1945] It will typically also require the controller to secure an *audit clause*, which either entitles the cloud customer to initiate its own audit (performed either by himself or by a trusted third-party) or guarantees periodic validation and certification by an independent third party.[1946]

947. CLOUD PROVIDER – In practice, the cloud provider will often determine the security features of his services in advance. The cloud provider should render these features transparent towards potential cloud customers, so that they can make an informed decision about whether or not to use the service.[1947] The information provided should be sufficiently detailed as to allow the customer to determine whether technical and organisational measures taken by the controller provide an appropriate level of security.[1948] In addition, the cloud provider should offer "*a sufficient level of information on the threats on and vulnerabilities of the CSP service and infrastructure and on the risk management decisions taken by the CSP*."[1949] Finally, the cloud provider should in principle notify the cloud customer in case of any security breach which affects the customer's data.[1950]

[1943] Article 17(1) of Directive 95/46.
[1944] Article 17(2) of Directive 95/46.
[1945] This risk assessment must cover not only risks presented by the processing itself (e.g., nature of the data, impact on data subject), but must also cover risks relating specifically to use of cloud computing services (e.g., loss of control or transparency). The risk analysis should also address specific data protection compliance risks, which concern mainly security obligation and international transfers (Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 19). For a detailed discussion of typical security objectives to be assessed: Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, 14-16 and D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 21 et seq.
[1946] See Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 22 and Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 11 and Sopot p. 5-6 for a more detailed discussion of audit requirements. See also Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 15 for a template audit clause.
[1947] B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1013.
[1948] Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 10.
[1949] Id. The Working Party considers that without such information, the he background for the customer to perform its own data protection risk management would not be adequate. (*Id.*)
[1950] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 21; D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p105 ENISA (cloud provider should notify customer of security breach).

948. SHARED RESPONSIBILITY IN PRACTICE – At a practical level, ensuring the confidentiality and security of personal data in the cloud is typically a shared responsibility between cloud providers and cloud customers.[1951] Different cloud providers have put forward different models of task distribution. Microsoft, for example, in its Whitepaper on Protecting Data and Privacy in the Cloud argues that:

> "*While providers are responsible for building services and features that facilitate compliance with applicable data protection and privacy regulations and standards, it is up to the customer to configure services and train their workers to use those services in a way that maintains compliance requirements for its industry and location. Also, though it is up to the provider to create strong operational controls to protect customer data in the cloud, it is up to the customer to use those controls in a way that limits unintended data sharing and access. Finally, the provider is responsible for demonstrating its commitment to data protection by obtaining certifications, sharing attestation reports, and signing agreements. However, it is the cloud customer's responsibility to verify that the provider's audit reports, certifications and other evidence meet its organisational data protection expectations."*[1952]

Amazon Web Services proposes a slightly different task model. A distinction is made between "security *of* the cloud" the cloud, which concerns the security of the underlying cloud infrastructure (hardware, networks, servers, location) and "security *in* the cloud", which concerns the security of applications, platforms and operating systems that run in the cloud. [1953] While the former is considered the responsibility of the cloud provider, the latter is considered the exclusive responsibility of the cloud customer. In the end, the actual distribution of tasks will depend to a large extent on type of cloud service offered (SaaS, PaaS or IaaS), as this determines the level of control which each party has over each layer of the software stack (hardware, operating system, middleware, software). ENISA has developed a comprehensive overview of the division of security-relevant roles and responsibilities in relation to each service model, noting that the actual division of responsibilities may vary widely between SaaS offerings and IaaS offerings.[1954]

[1951] See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 20.

[1952] Microsoft, "Protecting Data and Privacy in the Cloud", *Reactive Security Communications*, 2014, p. 10, available at http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf (last accessed 5 January 2015).

[1953] Amazon Web Services, *Whitepaper on EU Data Protection*, October 2015, p. 3-4, available at http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf (last accessed 5 January 2015).

[1954] See D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 66-68. A visual representation of a similar distribution of responsibilities is provided by Microsoft's "a data protection responsibility spectrum" (Microsoft, "Protecting Data and Privacy in the Cloud", *l.c.*, p. 10). See L. Badger, T. Grance, R. Patt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, *o.c.*, p. 5-1 et seq. for a detailed discussion of the control enjoyed the level of control which each party has over each layer of the software stack (hardware,

949. CONTRACTUAL BINDING – Pursuant to article 17(3) of Directive 95/46, the cloud provider should – as a minimum – be bound to (a) act only on instructions from the controller and (b) implement appropriate technical and organisational measures to ensure security of processing. The Article 29 Working Party has recommended that cloud contracts include a wide variety of additional provisions as "contractual safeguards for the controller-processor relationship".[1955] In particular, the Working Party recommends inclusion of terms describing:

1. the extent and modalities of instructions issued by the cloud customer to the cloud provider;
2. the specific security measures which shall be implemented by the cloud provider;
3. the subject and time frame of the cloud service;
4. extent, manner and purpose of the processing of personal data by the cloud provider, as well as the types of personal data processed.
5. conditions for returning or destroying personal data once the service has is concluded;
6. the duty of confidentiality of the cloud provider and his employees;
7. the obligation of the provider to support the customer in facilitating exercise of data subjects' rights to access, correct or delete their data;
8. the prohibition for the cloud provider to communicate data to third parties (subcontractors or other parties) unless provided for by contract;
9. a duty to notify the cloud customer in case of a security breach affecting the customer's data;
10. the list of locations where personal data may be processed;
11. the controller's rights to monitor and the cloud provider's corresponding obligations to cooperate;
12. the duty to inform the cloud customer prior to any changes to the service or implementation of additional functions (whereby the customer should at all times have the possibility to object to such changes or to terminate the contract, especially as far as sub-processing is concerned);
13. the logging and auditing of relevant processing operations that are performed by the cloud provider or subcontractors;
14. how government access request shall be dealt with (which in principle require prior notification to the cloud customer unless prohibited under criminal law to preserve the confidentiality of a law enforcement operation);

---

operating system, middleware, software). Appendix A offers an outline of the distribution of responsibilities between cloud providers and customers depending on the service model.

[1955] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 12

15. a general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.[1956]

950. SUB-PROCESSING – Cloud providers that act as processors may in practice subcontract certain services out to sub-processors.[1957] According to the Article 29 Working Party, the cloud provider (processor[1958]) may only do so with the agreement of the customer after informing the customer of "*the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC*".[1959] In addition, all relevant obligations applicable to the cloud provider should be made binding upon its subcontractors.[1960] The cloud customer should also be afforded the ability of contractual recourse against subcontractors in case of breach of contract.[1961]

951. ASSESSMENT – With the exception of article 16, Directive 95/46 only imposes obligations directly on controllers. Nevertheless, the Working Party envisages far-reaching information obligations for cloud providers acting as processors. The Working Party also envisages extensive contractual guarantees beyond the minimum provisions mentioned in article 17(3) of Directive 95/46. In practice, cloud customers (especially SME's) may find it difficult to negotiate such guarantees.[1962] By framing the recommended provisions as "*contractual safeguards of the controller-processor relationship*"[1963], the Working Party is seemingly nudging cloud providers to put in place the mentioned provisions in order to secure their processor status. In other words: to be considered a processor, it is not (or no longer) sufficient for a cloud provider to simply process "on behalf of" the cloud customer, the provider must also surrender itself to the authority of the customer with regard to relevant data protection aspects (if it wishes to retain its processor status).[1964] If the cloud provider uses personal data in a way that

---

[1956] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 12-14
[1957] *Ibid*, p. 9.
[1958] According to the CNIL, if the cloud provider controller acts as a joint controller, the provider is not required to obtain prior authorization from the customer but only has to inform the customer: see Commission Nationale de l'Informatique et Libertés (CNIL), *Recommendations for companies planning to use Cloud computing services*, *o.c.*, p. 8.
[1959] *Ibid*, p. 9
[1960] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 9-10. See also *supra*; nrs. 183 et seq. This obligation has since been codified by way of article 28(4) GDPR.
[1961] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 10. This could be arranged either by a third-party beneficiary right or by allowing the provider to sign the contract on behalf of the customer, making the latter a party to the contract (*Id.*).
[1962] See also J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 47.
[1963] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 12.
[1964] See also Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 8 ("*The CSP may cease to be considered as a processor, with all its consequences especially in terms of liability, in cases where the actions taken by the CSP exceeds by far the normal capacities of a data processor in view of its supposed absence of autonomy with respect to the*

breaches the contract, it will also be considered a controller in relation to these activities and may be held liable accordingly.[1965]

4.4 DATA SUBJECT RIGHTS

952. CLOUD CUSTOMER – The cloud customer must ensure that it is able to accommodate data subjects' rights of access, correction or deletion or blocking. The cloud customer must therefore verify the cloud provider does not impose technical and organisational obstacles which would prevent the customer from giving effect to data subject rights, including in cases when data is further processed by subcontractors.[1966]

953. CLOUD PROVIDER – A cloud provider (as processor) is not obliged to accommodate data subject rights. Strictly speaking, Directive 95/46 also does not require processors to cooperate with controllers in facilitating the exercise of data subject rights. Nevertheless, the Article 29 Working Party considers that the cloud provider must also support and assist the controller in complying with exercised data subjects' rights.[1967] The enforceability of this obligation depends, however, on the existence of a provision to that extent in the contract between cloud provider and customer. In cases where the provider acts as co-controller, the cloud provider is also directly responsible for accommodating data subject rights. If that is the case, the responsibilities for exercise of data subject rights should also be clearly allocated between the cloud provider and cloud customer.[1968]

4.5 INTERNATIONAL TRANSFERS

954. CLOUD CUSTOMER – Article 25-26 of Directive 95/46 generally prohibit controllers from transferring personal data outside the EU unless the country to where the data shall be transferred ensure an adequate level of protection. Absent a finding of adequacy, the controller must adduce "adequate safeguards" to ensure a continuous level of protection. In cases where the cloud provider is established outside the EU, has data centers outside the EU, or subcontracts to other processors established outside the EU, the cloud customer shall in principle be obliged to put in place additional safeguards

---

instructions of the controller."). See also B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1013.

[1965] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 14.

[1966] *Ibid*, p. 16

[1967] *Ibid*, p. 9. See also D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 105 and P. Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU", *l.c.*, p. 171.

[1968] Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 9.

(or ensure that safeguards are in place). Such safeguards may in particular take place in the form of contractual clauses or binding corporate rules.[1969]

955. CLOUD PROVIDER – The cloud provider should be transparent towards the cloud customer regarding all jurisdictions in which personal data may be processed (either by the cloud provider itself or its subprocessors).[1970] A list of locations in which the cloud service may be provided should be included in the contract.[1971] A cloud provider that engages in international transfers without the prior authorization of the cloud customer shall in principle be deemed a controller.[1972] Specifically, the Working Party considers that:

> "*The CSP may cease to be considered as a processor, with all its consequences especially in terms of liability, in cases where the actions taken by the CSP exceeds by far the normal capacities of a data processor in view of its supposed absence of autonomy with respect to the instructions of the controller. This may be the case, for example, where CSPs autonomously organise international transfers of data to respond to a law enforcement authority or state security's requests without seeking any involvement of the respective controllers.*"[1973]

956. ASSESSMENT – As with the obligation to ensure confidentiality and security, the Working Party seemingly leverages the "supposed absence of autonomy" of processors to require cloud providers to be transparent with regards to the locations of the data processing and to commit themselves to those locations by way of contract.

[1969] See Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 17 et seq. For more information regarding BCR's for processors see Article 29 Data Protection Working Party, "Explanatory Document on the Processor Binding Corporate Rules", WP 204 rev.01, adopted 19 April 2013, revised 22 May 2015, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf.

[1970] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 20. See also Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 7.

[1971] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 21

[1972] Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 8.

[1973] *Id.*

5 EVALUATION

957. OUTLINE – For some, cloud computing can be viewed as simply the next evolutionary step in IT outsourcing.[1974] Nevertheless, the cloud computing paradigm has put considerable pressure on the existing concepts of Directive 95/46. First, the specialized nature of certain cloud services can make it difficult to determine whether the cloud provider should be considered a controller or processor. Second, there is often an imbalance in the negotiating power between cloud providers and customers, which means that customer may not always be able the secure the appropriate guarantees. Third, the growing diversification in cloud computing services increases the number of actors involved in the processing of personal data, which may dilute the distribution of roles and responsibilities among the actors involved. Fourth, the argument has been made that certain actors in the cloud value chain should be labelled neither controller nor processor, especially in cases where the provider has no knowledge of the personal data being processed on its infrastructure. Finally, in cases where the user of the cloud service is covered by the personal use exemption, a gap in protection may arise.

5.1 THRESHOLD FOR CONTROL

958. CONCEPTUAL AMBIGUITY – Most scholars and regulators take the view that, at least as a point of departure, the provider of a cloud service should be considered a processor.[1975] Nevertheless, other scholars and regulators seem inclined to attribute certain cloud providers the role of controller, especially where SaaS providers are concerned.[1976] The confusion surrounding the status of certain cloud providers is attributable, at least in part, to the nature of the two criteria that give rise to control: purposes and means.

959. CLARIFICATION OF "PURPOSE" – According to the Article 29 Working Party, a processor by definition cannot be involved in the determination of the purposes of the processing.[1977] In case of SaaS, however, the service offered by the provider is usually designed with a particular use (i.e. "purpose") in mind.[1978] Certain applications, such as customer service management, intrinsically involve processing of personal data. Does the offering of a standard service intended for processing personal data amount to a definition of "purpose"? The Working Party's guidance on cloud computing is essentially silent on this issue.[1979] Scholars have answered this question in different ways.

[1974] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 4.
[1975] Cf. *supra*; footnote 1880.
[1976] Cf. supra; footnote 1881.
[1977] Cf. *supra*; nr. 92.
[1978] See also F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 10.
[1979] The Working Party merely notes that a cloud provider shall be deemed a controller if it uses personal data for its "own purposes". This reference to the "own purposes" of the cloud provider implicitly seem to refer to purposes other than the delivery of the service explicitly requested by the customer.

Mantelero and Determann, for example, argue that one of the reasons why cloud providers should not be viewed as controllers is because they offer their services without any interest in the data being processed or the uses made of these data.[1980] Gilbert, on the other hand, points to a number of Working Party opinions in which service providers have been deemed controllers even if they do not have a direct interest in the outcome of the underlying processing activities.[1981]

960. "PURPOSE" VS. "INTEREST" – The historical-comparative analysis of data protection law (undertaken in Part III of this thesis) offers some support to the argument that the concept of "purpose" coincides, to a large extent, with the concept of "interest". Traditionally, the controller has always been conceived of as the "beneficiary" of the processing: the data processing is carried out "on his behalf", "for his activities", or "for his purposes".[1982] Salom points out that the existence of an "interest" in the processing almost automatically excludes that the entity concerned may be considered a processor:

> *"Since data processors act on behalf of controllers, they have no personal interest in the outcome of the process they carry out (except the economic interest relating to the compensation agreed with the controller for the services provided, and their liability for the quality of these services); in fact, if data processors had any personal interest in the purposes sought in data processing, they would lose their status as data processor because they would stop acting on behalf of the data controller to act on their own behalf, for their own interest and, therefore, would not fit the definition of data processor provided under the Directive*".[1983]

961. PURPOSE AS FINALITY – While there exists a close relationship between the concepts of "purpose" and "interest", the two are by no means identical.[1984] The purpose of the processing refers to the finality of the processing, i.e. the *aims* or *objectives* pursued by the processing. Establishing the purpose of the processing of the processing can be achieved by asking the following questions: "*To what end are personal data being*

[1980] A. Mantelero, "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *l.c.*, section 3.1 ("*[…] the cloud provider receives the information to be processed in the interest of the user*") and L. Determann, "Data Privacy in the Cloud—Myths and Facts", *l.c.*, Myth 10 ("*[…] providers tend to offer a platform or software functionality as a service, without any interest, knowledge, or influence regarding data types and processing purposes*").

[1981] F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 9 et seq. (analyzing the Working Party's opinions on applicable law (WP 179), online social networks (WP 163), and SWIFT (WP 128)),

[1982] Cf. *supra*; nr. 624.

[1983] J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 178. See also T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", in B. Docquir and A. Puttemans (eds.), *Actualités du droit de la vie privée*, Bruylant, Bruxelles, 2008, p. 101 ("*L'utilité et le bénéfice du traitement ne le concernent pas directement*").

[1984] J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 181. An additional argument against equating "interest" with "purpose" is that article 7(f) of Directive 95/46 mentions both purpose and interest in the same sentence, thereby clearly indicating that the they carry a distinct meaning.

processed?" "*What is the output of the processing and what is the intended use of this output*?" Determining the purpose of the processing is therefore not the same as having an interest in the processing. The subtle distinction between "purpose" and "interest" is summarized eloquently again by Salom:

> "*The purpose of data processing refers to the objective or material result pursued through processing the personal data it focuses on, the information or the conclusion targeted as a result of processing the data of interest, or in the inferences made based on the personal data that are being processed. […] In contrast, the interests that are intended to be fulfilled through the data processing reveal an entirely subjective aspect, namely the project, business, or activity being developed and for which data processing is essential. The interests pursued by data processing are based on an intention, and are a completely volitional and abstract element for which data processing operations can be used as a necessary tool.*"[1985]

If a cloud provider has an interest in the outcome processing, it almost invariably means that the provider is also involved in the determination of the purposes of the processing (at least for those operations whereby it has an interest in the outcome of the processing). It can also be argued, however, that the cloud provider should be deemed a controller even where he has no direct interest in the processing, simply by virtue of its involvement in determining the output or material result of the processing.

962. CLARIFICATION OF "MEANS" – Cloud providers often determine large portions of the "means" of the processing (e.g., the hardware, operating system, and software applications).[1986] But is this sufficient to consider them controllers? The Article 29 Working Party accepts that processor(s) may enjoy a certain "margin of manoeuvre" in specifying how the processing shall be organized.[1987] Only if the processor determines the "essential" means of the processing would this imply its status of controller.[1988] The Working Party does not consider the choice for a particular hardware or software as determining "essential" means per se. Nevertheless, other aspects of the processing which are often determined by cloud providers (e.g., security measures, location of data, use of subcontractors, deletion processes, new service features, synchronisation services) may be considered as "essential" means.[1989] Yet deciding about these aspects

---

[1985] *Ibid*, p. 181. Salom further observes that Directive 95/46 consistently employs the terms purpose and interests with this subtle distinction in mind ("*In this sense, the Directive refers to the purposes of the data processing when regulating the information obligation in Articles 10 (c) and 11 (b), not obliging the data controller to inform about its interest in the data processing, and also makes several references to the purpose of different kinds of data processing in recitals (28), (30), and (37), and Article 4.1 (c). […] The Directive never refers to the 'interest of the processing' but to the 'interest of 'an entity or individual, referring always to a subjective intention in recitals 30, 42, 45, and Articles 7 (f), 8 (b), 13.1 (e), and 26.1 (c) and (e).*")

[1986] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 10.

[1987] Opinion 1/2010, p. 13-14.

[1988] *Ibid*, p. 14.

[1989] See also F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 9; W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 11. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data

of the processing apparently is not enough for the Working Party to consider the cloud provider as a controller. Indeed, the analysis in section 4 suggests that as long as the cloud provider clearly outlines the essential elements of the processing in advance (and does not draw outside these lines without additional agreement from the customer), the provider may retain its status as processor.[1990]

963. BALANCING TEST – To help distinguish between controllers and processors, the Article 29 Working Party has provided a range of additional criteria.[1991] In practice, the approach advanced by the Working Party seems to be more of a "balancing test" or "sliding scale" rather than a rigid adherence to existing criteria. As noted by Gilbert:

> *"The opinions issued by the Working Party show a sliding scale. The more the service provider follows the specific instructions of the client, the more chance it has to be deemed a data processor. On the other hand, the more the service provider has autonomy, and has the ability to make decisions regarding the data, the more likely it is that, at least with respect to these specific activities, the service provider would be deemed a data controller."*[1992]

Based on an analysis of key opinions of the Article 29 Working Party, Gilbert has developed a list of questions to help determine whether the cloud provider should, on the whole, be deemed a controller or processor.[1993] While the additional guidance of the

---

Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 12 ("*…the complexity of the technical means used in the cloud environment has now reached such a stage that it is necessary to add that the cloud client/data controller may not be the only entity that can solely determine the "purposes and means" of the processing. More and more often, the determination of the essential elements of the means, which is a prerogative of the data controller, is not in the hands of the cloud client. In this respect, the cloud service provider typically designs, operates and maintains the cloud computing IT infrastructure*")

[1990] Cf. *supra*; nr. 951.

[1991] For example in Opinion 1/2010, the Working Party mentions: level of prior instructions given (the greater the level of instruction, the more limited the margin of manoeuvre of the processor; monitoring of the execution of the service (a constant and careful supervision of compliance provides an indication of being in control of the processing operations); image given to the data subject; and expertise of the parties (if the expertise of the service provider plays a predominant role in the processing, it may entail its qualification as data controller) (Opinion 1/2010, l.c., p. 28). See also CNIL, "Les transferts de données à caractère personnel hors Union européenne", not dated, p. 11-12, available at https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf and CNIL, "Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques", September 2010, p. 14-15, available at https://www.cnil.fr/sites/default/files/typo/document/20100909-externalisation.pdf (last accessed 28 April 2016). See also *supra*; nr. 97.

[1992] F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 8. Later, Gilbert continues: "*The opinions issued by the Working Party show a sliding scale. At one end of the spectrum, a service provider that provides only basic services is a data processor. At the other end, a service provider that is "in control," e.g., has autonomy, retains the power to draft and change its contracts and policies, or provides added value for the processing of the data, should be deemed a "data controller," and should share with the customer the liability and risks associated with the processing of personal data.*" (*Ibid*, p. 12.)

[1993] See F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 12.

Working Party is useful, it also demonstrates that a number of grey areas remain, which may lead to divergent interpretations in practice.[1994]

5.2 CONTRACTUAL IMBALANCE

964. TAKE IT OR LEAVE IT – Small and medium-size enterprises often have a weak bargaining position when negotiating contracts with cloud providers.[1995] Public cloud services are typically offered on a "take it or leave" it basis, whereby the customer has little ability to influence the design or operation of the system.[1996] If the contract offered by the cloud provider is an accession contract, the cloud customer may be unable to secure the necessary assurances and safeguards which are expected from controllers (e.g., guarantees regarding security measures, data localisation, audits and limits on subcontracting).[1997]

965. CONTROL VS. MARKET DYNAMICS – The Article 29 Working Party has consistently held that the imbalance in contractual power between a small controller and a large service provider is not a justification for the controller to accept clauses or terms which are not in compliance with data protection law.[1998] A controller considering cloud services must simply choose a cloud provider that offers sufficient guarantees for compliance with data protection legislation.[1999] The problem of contractual asymmetry is therefore not an issue of conceptual ambiguity per se, but also an issue how of market dynamics that can lead to situation where certain cloud customers (especially SME's) are forced to choose from services which may not offer necessary guarantees. As noted by the EDPS:

> "*[T]he contractual asymmetry between service providers and clients […] may make it very difficult or even impossible for cloud clients acting as data controllers to comply with the requirements for personal data processing in a cloud computing environment. The asymmetry could also lead to an undesirable allocation of responsibility in relation to compliance with data protection law. If the qualification of data controller and processor does not appropriately reflect the*

[1994] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 11.
[1995] D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, *o.c.*, p. 98.
[1996] See e.g. R. Leenes, "Who Controls the Cloud?", *l.c.*, p. 8-9. See however also D. Catteddu and G. Hogben (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, November 2009, p. 98.
[1997] J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 47-48 and J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 11.
[1998] Opinion 1/2010, l.c., p. 26.
[1999] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 8

level of control over the means of processing, the responsibility for the protection of personal data even risks to evaporate with the use of cloud computing"[2000]

966. IMPROVING CLOUD CONTRACTS – Regulators have responded to the issue of contractual asymmetry in different ways. The Article 29 Working Party, for example, has mainly sought to leverage the obligations of the controller to stimulate transparency and contractual assurances on the part of cloud providers.[2001] The EDPS, on the other hand, seems to favour an approach whereby cloud providers were viewed as joint controllers, especially in case of SaaS applications.[2002] In both instances, the ultimate objective is to ensure the existence of appropriate contractual arrangements between cloud providers and cloud processors. The development of model contracts, codes of conduct and certification mechanisms could help to stimulate the adoption of more balanced cloud contracts which appropriately take into account data protection issues.[2003]

967. DIRECT OBLIGATIONS – A third approach, which was incorporated by the European Commission in its proposal for a General Data protection Regulation, is to increase the number of obligations directly incumbent upon processors.[2004] For example, article 30 of the draft proposal imposes the obligation to implement appropriate security measures on both controllers and processors, and article 31 expressly stipulates that the processor must notify the controller in the event of a data breach. Restrictions regarding international transfers have also been made directly applicable to processors.[2005] A major benefit of directly imposing obligations upon processors is that certain responsibilities can be allocated without being dependent on the existence of contract. Nevertheless, an effective division of responsibilities will most

---

[2000] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 6. See also W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 12-14 (noting that many providers do not even acknowledge processor status, let alone bind the provider to the elements required by article 17 of Directive 95/46).

[2001] Cf. *supra*; nrs. 938 et seq.

[2002] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, paragraph 55.

[2003] See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 25-26. See in this regard also European Commission, Commission Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts, *O.J.* 20 June 2013, C 174/6, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF.

[2004] See also *infra*; nrs. 1196 et seq.

[2005] In the final version of the GDPR, a number of obligations which are also be relevant to certain cloud providers (especially SaaS providers) have not been made directly applicable to processors. This is most notably the case for the principle of privacy by design and the obligation to undertake data protection impact assessments. Regarding the role that the principle of privacy by design can play in the development of cloud computing contracts see also Microsoft, "Protecting Data and Privacy in the Cloud", l.c., p. 4-5. See also *infra*; nrs. 1263 et seq.

likely still require a further specification of tasks in the form of a contractual arrangement.[2006]

5.3 NETWORKED DATA PROCESSES

968. MULTIPLICATION OF ACTORS – Cloud computing services are characterized by what Schwartz has termed "networked data processes".[2007] The cloud service offered by one provider might be produced by combining services from a range of other providers, which together realise a particular outcome.[2008] Another way to think about cloud services is in terms of "modular units", whereby different functions and operations can be assembled, pulled apart and reassembled as needed.[2009] The result is an environment which involves a growing number of actors, whereby each actor is involved in the processing to varying degrees, possibly at different levels of the software stack (hardware, operating system, middleware, software).[2010]

969. MULTIPLICATION OF CONTROLLERS? – One way to respond to the increased diversification of processing services is to apply the concept of control with more granularity. Instead of trying to squeeze certain cloud providers into the (increasingly ill-fitting) jacket of "processor", both provider and customer are treated as a "controllers" - but only with respect to those decisions and operations over which it has effective control.[2011] A major benefit of this approach is that it can lead to an allocation of responsibilities that reflects the actual influence over processing activities.[2012] An immediate consequence of such an approach, however, is a multiplication in the number of "controllers" involved whenever cloud services are used. Without appropriate incentives, there is also a risk that providers do not properly distribute tasks among each other, thereby decreasing the overall level of protection for data subjects.

970. UNINTENDED CONSEQUENCES? – The multiplication of controllers was an issue considered by the Article 29 Working Party in its Opinion 1/2010:

> "*[…] multiplication of controllers may […] lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing.*"[2013]

[2006] See e.g. Amazon Web Services, "Whitepaper on EU Data Protection", *l.c.*, p. 3-4 (distinguishing between security "in" and security "of" the cloud). See also *supra*; nr. 948.
[2007] P. Schwartz, "Information Privacy in the Cloud", *l.c.*, p. 1630.
[2008] Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 5
[2009] P. Schwartz, "Information Privacy in the Cloud", *l.c.*, p. 1634.
[2010] See also *supra*; nrs. 916 et seq.
[2011] See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, paragraph 55.
[2012] *Id.*
[2013] Opinion 1/2010, *l.c.*, p. 24.

The principle of transparency of processing is a core principle of data protection law. It underlies articles 10 and 11 of the Directive, which specify inter alia that the data subject must in principle be informed of the identity of the controller and/or his representative. The more controllers involved, the more identities will need to be communicated to the data subject, which some would argue can diminish the transparency of processing. But is this really an issue of how the concept of "controller" is applied? Or is the issue caused by the manner in which the duties regarding transparency towards data subjects are currently framed?[2014] A more significant issue is whether the multiplication of controllers might render the distribution of responsibilities more opaque, including towards data subjects. But as long as the data subject has the ability to fully exercise his rights towards the cloud customer for the whole of the processing[2015], it would appear that the multiplication of controllers would not adversely impact the data subject, on the contrary. The recourse options of data subjects would actually increase.[2016] When considering this path, one should of course also carefully consider the other provisions of the Directive that hinge upon the correct qualification of the actors involved in the processing. After all, the qualification of an actor as either a controller or processor has implications beyond the allocation of responsibility and risk.[2017] This issue will be revisited later on in this thesis.[2018]

5.4 HOSTING SERVICES

971. CLOUD PROVIDERS AS HOSTS? – Article 14 of the E-Commerce Directive describes "hosting services" as services consisting of the storage of information provided by the recipient of the service. Seeing as the majority of cloud providers store personal data on behalf of their customers, Kuan Hon and others have argued that cloud providers (especially PaaS and IaaS providers) should be considered as "hosts".[2019] The main motivation for their argument appears to be the favourable liability regime which has been granted to hosts. Under article 14, hosts are in principle exempted from liability in relation to information stored at the request of their customers, as long as the provider does not have actual or constructive knowledge of the unlawful character of the information stored at the request of the recipient of the service.[2020]

[2014] Moreover, in its opinion on cloud computing, the Article 29 Working Party also expressly considered that cloud customers should also, as a matter of good practice, inform data subjects of the (sub)processors providing cloud providers (Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 6), which would mean that data subjects are in any event expected to be provided with information about identity of the cloud providers involved.

[2015] The cloud customer as controller would remain accountable for his decision to entrust the data processing to a particular cloud provider (as the customer exercised effective "control over this decision").

[2016] If the data subject has reason to believe that the processing at issue resides under the (co)control of the cloud provider, he or she would be able to exercise his rights against both the cloud customer and cloud provider(s).

[2017] Cf. *supra*; nrs. 188 et seq.

[2018] Cf. *infra*; nrs. 1132 et seq.

[2019] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, in particular at p. 17 et seq.

[2020] See article 14(1)a of Directive 2000/31/EC

972. THE "CLOUD OF THE UNKNOWING" – To support their argument, Kuan Hon and others point out that many cloud providers, especially infrastructure providers, do not have any knowledge or awareness of the fact that their systems are used to process personal data.[2021] They also point out that there are situations where the cloud provider may not even be able to determine whether the data processed using its infrastructure is personal in nature (e.g., in case of encrypted or anonymised data).[2022] In such situations, they argue that cloud provider should not even be considered a "processor", but should instead be exempted from compliance with data protection requirements altogether:

> *"A cloud provider whose services are used to process data on behalf of a consumer or business customer, but who does not know that the data are 'personal data', or who knows the data's status but has no access to the data it processes, should not be a 'processor' for the purposes of the DPD, because a processor, according to the definition, 'processes personal data'. Thus such a provider should not be subject to any data protection obligations."*[2023]

The hosting exemption would only apply, however, insofar as the necessary conditions are met:

> "*Any such exemptions should of course be subject to similar provisions as to the loss of immunity, and corresponding imposition of data protection obligations as controller or processor, should the service provider acquire the relevant knowledge and/or access.*"[2024]

973. E-COMMERCE VS. DATA PROTECTION – A cloud provider that stores personal data on behalf of its customers can, as a matter of principle, be considered a hosting provider. The E-Commerce Directive, however, excludes a number of matters from its scope. Most relevant here is the exclusion contained in article 1(5)b, which provides that the E-Commerce Directive shall not apply to *"questions relating to information society services covered by Directive 95/46* [...]".[2025] A literal reading of article 1(5)b suggests that the liability exemptions provided in that Directive should not be applied in cases concerning the responsibilities of "controllers" or "processors", as these matters are regulated by Directive 95/46.[2026] This would imply that, even if a cloud provider could in

---

[2021] *Ibid*, p. 18-19 and p. 27.

[2022] *Id.* (""*[I]t is arguable that infrastructure providers are not even 'processors', particularly where they are used only for processing power. It is more difficult to do so where the service provided consists of or includes persistent storage of data, in other words where the provider acts as a data host. However, the provider will often not know the nature of data stored with it, so it seems problematic that its status should depend on what data its customer decides to store and how well the customer encrypts or anonymises the data.*").

[2023] *Ibid*, p. 28. See also p. 18 ("*We therefore suggest that mere hosting of data, without knowledge as to its 'personal data' nature, should not render the provider a processor, and even more so with encrypted data: the cloud of unknowing should not be the cloud of 'processing'. We believe an exemption or exception to data protection laws is justified here.*")

[2024] *Id.*

[2025] Article 1(5)b of Directive 2000/31.

[2026] Contra: G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law* 2014, Vol. 21, No. 3, p. 574 ("*[Article 1(5)b of the eCommerce Directive] has sometimes been read as excluding violations of data protection from*

principle benefit from one of the exemptions contained in the E-Commerce Directive, it would not automatically exempt the provider from liability under the Data Protection Directive.[2027] The General Data Protection Regulation will seemingly reverse this position. Article 3(2) specifies that the Regulation "*shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive*".

974. ASSESSMENT – The issue of whether or not cloud providers can be qualified as "hosts" may, in many cases, be of only limited practical relevance. There are mainly two reasons for this. The first reason is that the liability exemption for hosts is predicated upon an absence of knowledge. Certain cloud services (especially SaaS) services are simply intended to process personal data. As a result, the cloud provider cannot reasonably claim to be unaware of the fact that processing of personal data is taking place. Moreover, if the cloud customer complies with his obligation to ensure an appropriate contractual binding of the provider (cf. *supra*), the latter will by definition have knowledge of the fact that his service is used to process personal data (even in case of PaaS or IaaS services). Hence the cloud provider would no longer be "unknowing" of the nature of the content or activity. Second, in situations where the cloud provider does not have actual or constructive knowledge of the fact that personal data are being processed (e.g., if the cloud customer failed to obtain appropriate safeguards), the provider should be able to argue that the event giving rise to the damage cannot reasonably be attributed to him.[2028] Therefore, the practical impact in terms of actual liability exposure of most cloud providers may be quite limited.[2029] From the provider's perspective, however, the formal recognition of the applicability of the hosting regime may provide additional legal certainty and help it to assess its legal risks when offering cloud services to EAA-based cloud customers.

5.5 PERSONAL USE EXEMPTION

975. CONSUMER SERVICES – Cloud services are not only used by businesses and governments, but also by individuals. Individuals who make use of cloud services in a purely personal capacity shall in principle be exempted from compliance in accordance

---

the e-commerce immunities, so that providers would be liable when transmitting or hosting data uploaded by third parties in violation of data protection law. On the contrary, this provision can be understood as only meaning that the obligations concerning data protection remain only those established by the Data Protection Directive, a statement that is fully compatible with the immunity of intermediaries for third parties' violations of such obligations.") See also M. Peguera, "The Shaky Ground of the Right to Be Delisted", (Draft, August 2015), p. 31 et seq., available at http://ssrn.com/abstract=2641876 (last accessed 25 August 2015) ("*[…] a reading of Art. 1(5)(b) more consistent with the rest of the Directive might conclude that it does not intend to limit the scope of the safe harbors.*").

[2027] This interpretation is further supported by recital (14) of the E-Commerce Directive which states that "*the protection of individuals with regard to the processing of personal data is solely governed by Directive 95/46 […] which is fully applicable to information society services*".

[2028] See article 82(3) of the GDPR.

[2029] In the same vein (regarding search engines): B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, 60-62.

with article 3(2) of Directive 95/46 (unless the cloud service is used to make data available to an indefinite number of people).[2030]

976. PROTECTION GAP - In its Opinion on the future of privacy, the Article 29 Working party noted that a gap in protection may arise when individuals that consume cloud computing services.[2031] If the individual is exempted from compliance under the personal use exemption, Directive 95/46 arguably also does not apply to the cloud provider, insofar as the provider may not be deemed a controller.[2032] As result, any personal data entrusted by the individual to the cloud provider (which may concern either the individual or third parties) would in principle not benefit from the protections provided by Directive 95/46.[2033]

977. BASELINE OBLIGATIONS – To address this gap in protection, the Article 29 Working Party recommended that the providers of services to private individuals be required to provide certain safeguards regarding confidentiality and security, regardless of whether the activities of the customer fall within the scope of Directive 95/46.[2034] As indicated earlier, the General Data Protection Regulation has imposed obligations directly upon processors.[2035] Moreover, recital (18) explicitly clarifies that the Regulation applies to processors which provide the technical means for processing personal data for personal or household activities. The combination of these provisions should be sufficient to address the gap in protection which might otherwise exist in cases where the customer of a cloud service entrusts personal data to a cloud provider.[2036]

[2030] Cf. *supra*; nrs. 868 et seq.

[2031] Article 29 Data Protection Working Party and Working Party on Police and Justice, "The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data future of privacy", WP 168, 1 December 2009, p. 18, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[2032] *Id.* See also P. Hustinx, European Data Protection Supervisor, Data protection and Cloud Computing under EU law, Third European Cyber Security Awareness Day, European Parliament, 13 April 2010, p. 5, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf (last accessed 11 January 2015).

[2033] See also J.G.L. van der Wees, "De verantwoordelijke en de bewerker in de cloud", *l.c.*, p. 112; B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1006 and J.-M. Van Gyseghem, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *l.c.*, p. 3.

[2034] Article 29 Data Protection Working Party and Working Party on Police and Justice, "The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data future of privacy", *l.c.*, p. 18.

[2035] Cf. *supra*; nr. 609.

[2036] Absent the protection of the General Data Protection Regulation, individual consumers of cloud computing services would in principle only be able to benefit from the contractual promises made by the cloud provider (unless the cloud provider acts as a controller). (B. Docquir, "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *l.c.*, p. 1006).

Chapter 5 INTERNET SEARCH ENGINES

1 INTRODUCTION

978. INFORMATION LOCATION TOOLS – Internet search engines facilitate the location and retrieval of information. Specifically, they help their users to find relevant content amidst the abundance of content that is available online.[2037] Without these services, locating relevant information on the web would often be a challenge.[2038] With the help of search engines, however, information on just about any topic can be retrieved with considerable ease.

979. BENEFITS – The societal benefits of internet search engines are tremendous. On a daily basis, people all over the world use search engine services for various activities, such as shopping, research and entertainment. People also use search engines to get in touch with new ideas or to stay abreast of global developments. It is therefore fair to say that search engines play a pivotal role in today's information society. They also promote fundamental values such as freedom of expression and access to information. As observed by the Committee of Ministers of the Council of Europe:

> "*Search engines enable a worldwide public to seek, receive and impart information and ideas and other content in particular to acquire knowledge, engage in debate and participate in democratic processes.*"[2039]

980. PRIVACY IMPACT – Notwithstanding their tremendous benefits, internet search engines have also roused numerous privacy concerns. A distinction can be made between two sets of concerns: those relating to (1) the users of search engine services and those relating to (2) search targets.[2040] The first set focuses on the privacy interests of people who use internet search engines. Individuals reveal a lot of information about themselves when searching for information online: about their personal interests, their

---

[2037] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 5.

[2038] As Solove put it: "*Without search engines, the Internet would be an endless expanse of digital babble, and finding any particular piece of information would be akin to locating a specific grain of sand in the Sahara Desert.*" (D.J. Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, 2007, New Haven, Yale University Press, p. 9.)

[2039] Council of Europe, Recommendation of the Committee of Ministers to member States on the protection of human rights with regard to search engines, CM/Rec(2012)3, Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies, paragraph 1, available at https://wcd.coe.int/ViewDoc.jsp?id=1929429.

[2040] See e.g. O. Tene, "What Google Knows: Privacy and Internet Search Engines", *Utah Law Review* 2008, no. 4, p. 1440 et seq., available at http://www.epubs.utah.edu/index.php/ulr/article/viewFile/136/118?origin=publication_detail (last accessed 26 February 2013).

travel plans, their political beliefs, their sexual preferences, their medical conditions, etc. In fact, the data contained in a search-query log can be far more revealing than the contents of a private email or telephone conversation.[2041] The second set of concerns focuses on the privacy interests of "search targets". Internet search engines have made it relatively easy to find out information about just about anyone. By using a search engine, one can easily aggregate personal data which would otherwise remain dispersed across company websites, newspaper articles, social networking pages, blogs, etc. Internet search engines have, in other words, significantly reduced the transaction costs of compiling a comprehensive profile about a specific person.[2042] As a result, people have become increasingly concerned with the information to which search engines refer.

981. A RIGHT TO BE DELISTED? – Due to their impact, the providers of internet search engines are often confronted with requests to remove certain references from their search results. For example, a private individual might ask a search engine to stop referring to one or more web pages which contain personal data about them. The removal of references to harmful or privacy-intrusive content from search results can offer considerable relief for the affected individuals. At the same time, such a mechanism would give rise to a number of questions: do search engine providers have an obligation to accommodate such requests? Does it make any difference whether the content in question was lawfully published or not? Should a search engine operator be charged with drawing the balance between freedom of expression and privacy? These questions were at the heart of *Google Spain*[2043], a case decided by the Court of Justice on 13 May 2014.

982. SCOPE LIMITATION – The objective of this chapter is to analyse how the EU data protection framework relates to the activities of internet search engines. In the interest of brevity, this chapter will limit itself to analysis of the processing of personal data found on web pages and in search results. Personal data which is collected by internet search engines directly from their users are outside the scope of this chapter. This issue has already been treated extensively by scholars[2044] and regulators[2045], and is also less relevant to the research question of this thesis.

[2041] *Ibid*, p. 1442-1443.

[2042] *Ibid*, p. 1440. Without search engines, the visibility of much of these data would remain limited: even though they might be publicly accessible, uncovering and compiling all of these data would often be difficult and resource-intensive. (*Id.*)

[2043] Judgement in *Google Spain* C-131/12, EU:C:2014:317.

[2044] See e.g. O. Tene, "What Google Knows: Privacy and Internet Search Engines", *l.c.*, p. 1140-1464 and E. Kosta, C. Kalloniatis, L. Mitrou and E. Kavakli, "Search Engines: Gateway to a New 'Panopticon'?", in S. Fischer-Hübner a.o. (eds.), *Trust, Privacy and Security in Digital Business*, Lecture Notes in Computer Science Volume 5695, 2009, p. 11-21.

[2045] See e.g. International Data Protection and Privacy Commissioners' Conference: Resolution on Privacy Protection and Search Engines, 28th edition, 2-3 November 2006, London, accessible at http://privacyconference2011.org/htmls/adoptedResolutions/2006_London/2006_L4.pdf; Agencia Espanalo de Protección de Datos (Spanish Data Protection Agency), "Statement on Internet Search Engines", p. 4 et seq, 1 December 2007, accessible at https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracio

983. TERMINOLOGY – For purposes of simplicity, the terms "search engine" and "search engine provider" shall be used as synonyms for the terms "internet search engine" and "internet search engine provider" respectively. The reader should note, however, that the term "search engine" is also used in a more generic sense, i.e. to refer to any technical component designed to discovery of resources within a (open or closed) information system. In the context of this chapter, the term "search engine" is used to refer to information retrieval systems designed to facilitate the location and retrieval of content which is publicly accessible via the Internet.

984. OUTLINE – This chapter will begin by identifying the main actors involved in the publication and retrieval of online information. Next, it will analyse the legal status ("role") of each actor, as interpreted by regulators, scholars and courts. After that, we will describe the main responsibilities of each of these actors in relation to their processing of personal data found on webpages.

985. ACKNOWLEDGEMENT – Substantial portions of this chapter consist of parts of a joint research paper written together with two of my colleagues.[2046] The parts reproduced here correspond, for the most part, with my personal contributions to this paper. However, the entire paper was a joint work and therefore their contributions should be duly noted. Explicit references to the joint paper are therefore also made throughout this chapter.

2 ACTORS

986. SELECTION CRITERIA – The current inventory of actors is based on a literature study of academic publications and regulatory guidance concerning internet search engines.[2047] A common denominator among the selected entities is that they

(1) process personal data which is (being) made publicly accessible via the Internet and/or

(2) are instrumental in the retrieval of such data.

---

n_aepd_buscadores_en.pdf; Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines", WP 148, 4 April 2008, p. 7 et seq., accessible at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf (all URLs last accessed 27 February 2014).

[2046] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *ICRI Working Paper Series*, Working paper 15/2013, September 2013, 74 p.

[2047] Although other sources have been consulted as well, the primary sources of reference were: J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, Academisch Proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam, defended on 23 March 2012, 357 p., available at http://dare.uva.nl/document/2/104098 (last accessed 12 January 2015); M.L. Boonk, *Zeker over zoeken? Naar een juridisch kader voor verichtingen van zoeksystemen met betrekking tot via internet beschikbare open content*, 2013, Zutphen, Uitgeverij Paris, 466 p.; Agencia Espanalo de Protección de Datos, "Statement on Internet Search Engines", *l.c.*, 15 p. and Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines", *l.c.*, 29 p.

987. ACTORS OVERVIEW – The following five actors may be considered as being particularly relevant to the availability, location and retrieval of personal data online:

(1) Search engine providers;

(2) Website publisher;

(3) Content providers;

(4) End-users; and

(5) Infrastructure Service providers.

988. VISUAL REPRESENTATION – The aforementioned actors interact with each other in a variety of ways. The following figure provides a - highly simplified - representation of how these actors typically interact with one and other to facilitate the retrieval of data contained on publicly available websites. It is intended to be conceptual rather than factual.

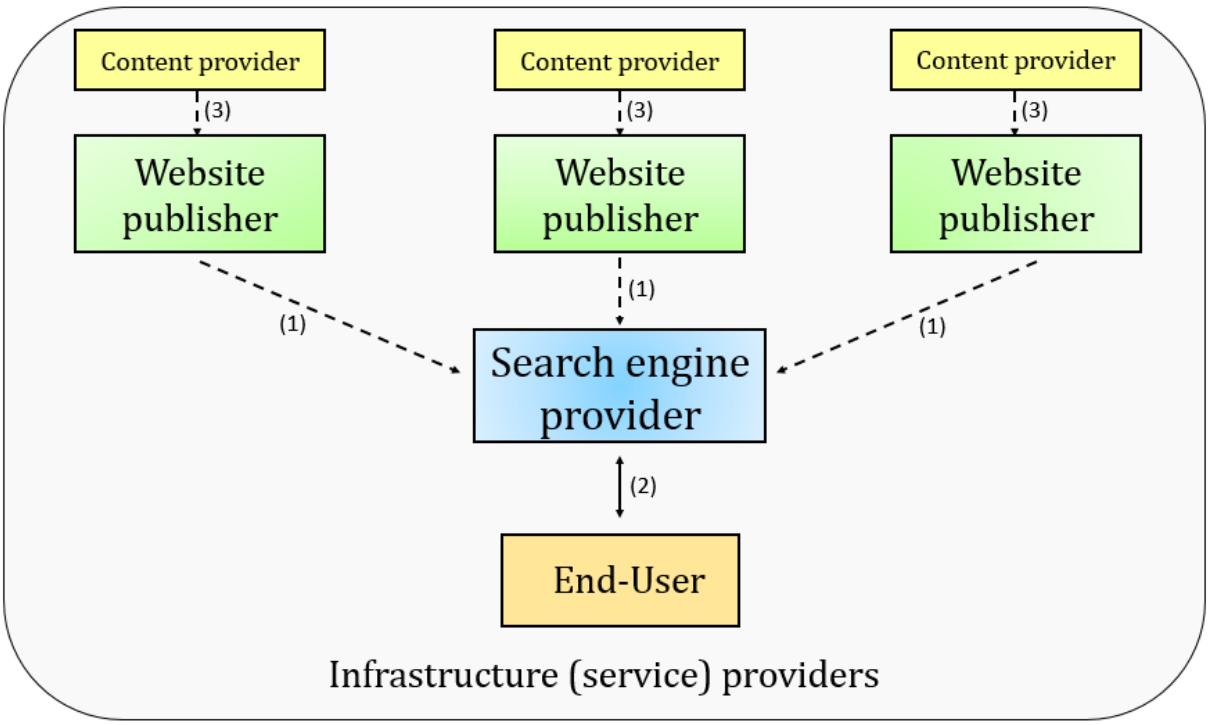

Figure 6 – Main actors internet search engines

989. LEGEND – The arrows in Figure 6 indicate that an exchange of personal data is taking place. Exchanges of personal data which are relevant to our current analysis our mainly uni-directional (with the exception of the interaction between end-users and the search engine provider). Solid black arrows were used to depict data exchanges in which the end-user is actively involved at the moment of delivery of the search engine service. Dashed grey arrows depict the transfers of personal data prior to delivery of the search

engine service. Over the following sections, a brief description is provided of each of the actors and interactions displayed in Figure 6.

2.1 *SEARCH ENGINE PROVIDER*

990. MAIN CHARACTERISTICS – In the context of this chapter, a search engine provider is understood as an entity that offers an information retrieval system for online content.[2048] These services are typically made available to the public at large at no monetary cost. The primary source of revenue for the providers of such search engines is derived from advertising.[2049]

991. PROCESSING ACTIVITIES – Search engine providers undertake a range of technical operations in order to provide their users with the search functionality. The following paragraphs will outline, by way of illustration, how search engine provider Google has described the operation of its search engine service. Similar operations are, however, undertaken by other search engine providers. Google identifies the following sets of operations[2050]:

(1) crawling;

(2) indexing;

(3) algorithmic analysis;

(4) retrieval;

(5) ranking; and

(6) fighting spam.

992. CRAWLING – "Crawling" is generally understood as the use of software programs that make requests for online material.[2051] These programs, also referred to as "crawlers" or "spiders", are configured to look for information on the Internet, "*according to a set of criteria which tell it where to go and when*".[2052] According to Google, its spiders

---

[2048] Based on J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 41. See also the definition provided by M.L. Boonk, who defines a search engine as "*a system which assists end-users in finding relevant information on the internet*" (personal translation) (M.L. Boonk, *Zeker over zoeken?, o.c.*, p. 36).

[2049] OECD, *The Economic and Social Role of Internet Intermediaries*, 2010, Paris, OECD Publishing, p. 12, available at http://www.oecd.org/internet/ieconomy/44949023.pdf (last accessed 27 February 2014)

[2050] See Google, "How search works – the Story", available at http://www.google.com/insidesearch/howsearchworks/thestory/ (last accessed 17 May 2013). See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 11-12.

[2051] J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 41. See also http://answers.google.com/answers/threadview/id/33696.html (last accessed 17 May 2013).

[2052] *Ibid*, p. 42-42.

"*start by fetching a few web pages, then they follow the links on those pages, and fetch the pages they point to, and follow all the links on those pages [...] and so on [...] until we've indexed a pretty big chunk of the Web*".[2053]

993. INDEXING – Once the relevant web pages have been fetched (i.e. a copy has been collected), the content of these pages is analysed and "parsed"[2054] for purposes of indexation.[2055] Google compares its search engine index to an index found in the back of a book, in that it "*includes information about words and their locations*".[2056] It is this index which is consulted when a search engine user enters a search query.[2057]

994. ALGORITHMIC ANALYSIS – As a user enters a search term, the search engine provider may try to gain a better understanding of what the user is looking for by analysing the search terms. For example, the provider might compare the entered search terms not only to keywords, but also to synonyms of that word. It may also check for common spelling mistakes or consider translations. A feature advertised by Google is its so-called "Knowledge Graph", a tool designed to map out the relationships between real-world objects (e.g., "Benjamin Franklin" and "Philadelphia") with a view of enhancing users' search experiences.[2058] Google also provides an "autocomplete" function, whereby it suggests possible search queries based on the information users have begun typing in

---

[2053] Matt Cutts (Google Quality Group Engineer), *How Search Works*, s30-s44, available at http://www.youtube.com/watch?v=BNHR6IQJGZs (last accessed 17 May 2013).

[2054] See J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 43 ("*The parser is the processing tool between the crawler and the index.* [...] *The pieces of content the crawler finds are not the same in size, sort, language, code, and other characteristics, so the parser need to normalize them for the index. It also extracts a number of related data and meta-data that can be useful for the search engine's technology*").

[2055] See also U. Kohl, "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)", *International Journal of Law and Information Technology* 2013, p. 5. Google states that it uses a "knowledge graph" to sort pages "*by their content and other factors*" (http://www.google.com/intl/en/insidesearch/howsearchworks/thestory/index.html). For more information on knowledge graphs and structural parsing see L. Zhang, *Knowledge Graph Theory and Structural Parsing*, PhD Thesis, University of Twente, 2002, available at http://doc.utwente.nl/38647/1/t0000020.pdf (last accessed 17 May 213).

[2056] See http://www.google.com/intl/en/insidesearch/howsearchworks/crawling-indexing.html (last accessed 17 May 2013). This is of a course a somewhat simplified representation: while keywords and references may be the basic elements of the index, a search engine's index also contains additional (meta-)information, which may for example be used to apply the ranking algorithms (J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 43).

[2057] "*[W]hen you do a Google search, you aren't actually searching the web, you're searching Google's index of the web*" (Matt Cutts (Google Quality Group Engineer), *How Search Works*, *o.c.*, s17-23). See also the Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 34: "*[S]earch results displayed by an internet search engine are not based on an instant search of the whole World Wide Web, but they are gathered from content that the internet search engine has previously processed. This means that the internet search engine has retrieved contents from existing websites and copied, analysed and indexed that content on its own devices. This retrieved content contains personal data if any of the source web pages do.*"

[2058] See e.g. Google, "Introducing the knowledge graph", 2012, available at http://www.youtube.com/watch?v=mmQl6VGvX-c (last accessed 17 May 2013).

the search box (e.g., a user typing "New York" might see suggestions for "New York Times" or "New Yorker").[2059]

995. RETRIEVAL AND RANKING – The search query, together with the provider's "interpretation" of it, is then used to consult the search engine's index. This exercise typically yields a large number of possible results. Not all results are equal, however. In determining the order of results, search engine providers apply what is commonly referred to as a "ranking algorithm". Google's ranking algorithm reportedly includes over two hundred factors, such as "site and page quality"[2060], "freshness", "user context" (e.g. location, web history), etc.[2061] A search engine provider might also, either autonomously or on the basis of user settings, filter out certain results based on their content (e.g., by filtering out what it believes to be "adult" images or content which has been reported as being "offensive").[2062] In addition, a search engine provider might also have a policy to "downgrade" certain types content, either manually or automatically (e.g. because it considers the website to be engaged in "spam").[2063]

996. USER DATA VS. THIRD-PARTY DATA – Personal data processed by search engines are typically divided into two categories: user data and third-party data.[2064] *User data* comprises all data relating to the individuals who use a particular search engine - in their capacity of users. These data are either (a) actively provided by the user to the search engine provider; (b) derived from his or her use of the service; or (c) obtained from other sources.[2065] *Third-party data*, on the other hand, refers to data about individuals which is drawn from (other) websites and displayed in the results pages of search engines.[2066] For example, if a newspaper article or blog post references an individual by name, this name might be included in a page description (or "snippet"[2067])

[2059] See Google, "Autocomplete", accessible at https://support.google.com/websearch/answer/106230?hl=en (last accessed 12 January 2016).

[2060] The "quality" of a website or page is determined by a variety of "signals" which are used to infer the trustworthiness, reputability or authority of a site (http://www.google.com/intl/en/insidesearch/howsearchworks/thestory/index.html). One of these signals is "PageRank", an algorithm which determines the relevancy of a webpage by looking inter alia at the number of times it is linked to by other web pages. (U. Kohl, "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)", *l.c.*, p. 5.)

[2061] http://www.google.com/intl/en/insidesearch/howsearchworks/thestory/index.html

[2062] For an example see Google's "SafeSearch" https://support.google.com/websearch/answer/510?hl=nl

[2063] See e.g. http://www.google.com/intl/en/insidesearch/howsearchworks/fighting-spam.html. For a more general overview of Google's policies affecting the search results it yields see http://www.google.com/intl/en/insidesearch/howsearchworks/policies.html.

[2064] Agencia Espanalo de Protección de Datos (Spanish Data Protection Agency), "Statement on Internet Search Engines", *l.c.*, p. 1.

[2065] Examples include IP addresses, user preferences, clickstream data, user names (where applicable), etc.

[2066] Agencia Espanalo de Protección de Datos (Spanish Data Protection Agency), "Statement on Internet Search Engines", *l.c.*, p. 2-3.

[2067] Google describes "snippets" as "*small previews of information, such as a page's title and short descriptive text, about each search result*" (http://www.google.com/intl/en/insidesearch/howsearchworks/algorithms.html). See also the Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 35 ("*internet search engines often display additional content alongside the link to the original website. There can be text extracts, audiovisual content or even snapshots of the source web pages. This preview information can be at*

displayed on the results page. As explained earlier, this chapter will only analyse the processing of such third-party data.[2068]

997. DATA FLOWS – Arrows (1) in figure 6 depict the collection of personal data that takes place when internet search engines crawl the web. Arrow (1) is uni-directional as crawling in principle involves only the collection of personal data, not disclosure of personal data. Arrow (2) depicts the interaction between the end-user and the provider of the search engine service. Arrow (2) is bi-directional because (a) the results presented by the search engine operator may include personal data and (b) the search queries entered by the user may include personal data.

2.2 WEBSITE PUBLISHERS AND CONTENT PROVIDERS

998. MAIN CHARACTERISTICS – In the context of this chapter, a website publisher is understood as the natural or legal person that makes one or more webpages publically accessible through the internet. Content included in a publically accessible webpage may be authored by the website publisher, by a third-party ("content provider"), or both. In other words, it is possible that the role of publisher and content provider coincide, but this is not necessarily the case.

999. DATA DISCLOSURE – There are several ways in which website content can wind up in the index of a search engine. The most common way is by simply posting the content online and waiting for the search engine's crawlers to come by and include it.[2069] In this regard, it is important to note that the publisher of a website can signal to search engines it does not wish for its pages to be indexed.[2070] The publisher can do this through the so-called *Robots Exclusion Protocol*, a protocol whereby the administrator of a website stores a file ("robots.txt") on the website's server specifying an access policy for web robots (e.g., web crawlers used by search engines).[2071] Specifically, the robots.txt file can be used to specify for which types of robots ("user-agent") the website publisher wishes to "disallow" access.[2072] Absent such specification, it is assumed that

---

least in part retrieved from the devices of the internet search engine service provider, and not instantly from the original website. This means that the service provider actually holds the information so displayed").

[2068] In other words: our analysis of the role and responsibilities of search engines under data protection law only concerns the processing at issue in *Google Spain* and does not pertain to the data protection obligations which search engines have in relation to their users (in their capacity as users).

[2069] J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 53. Other ways include participation in paid placement programs or other contracts between website publishers and search engine providers. (*Id.*)

[2070] X. "About /robots.txt", not dated, accessible at http://www.robotstxt.org/robotstxt.html (last accessed 12 January 2016).

[2071] M. Koster, "A Standard for Robot Exclusion", not dated, available at http://www.robotstxt.org/orig.html (last accessed 12 January 2016).

[2072] *Id.* See also Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraphs 41-42. ("*Source web pages are kept on host servers connected to internet. The publisher of source web pages can make use of 'exclusion codes' for the operation of the internet search engines. Exclusion codes advise search engines not to index or to store a source web page or to display it within the search*

the website publisher wishes for all its pages to be indexed.[2073] Website publishers can actually also try to optimise the way in which search engines include them in their search results, for example by using page description metatags.[2074]

1000. DATA FLOWS – Arrow (1) depicts the disclosure of data by website publishers to internet search engines. Arrow (3) depicts the disclosure of data from content providers to website publishers.

2.3 END-USERS

1001. MAIN CHARACTERISTICS – End-users are natural persons who make use of internet search engines to locate relevant information online. Search queries performed by end-users can be categorized into three broad categories, namely "informational", "navigational" and "transactional".[2075] When the user simply wants to find information about particular topic which is presumed to be available online, the search query is considered "informational".[2076] A search query is considered "navigational" if the end-user makes use of a search engine to find a specific website which he or she knew (or assumed) to be present on the web.[2077] Finally, a search query is "transactional" if the end-user aims to reach a destination where further interaction would take place, such as making a purchase.[2078]

1002. DATA DISCLOSURE AND COLLECTION – In order to be provided with the most relevant search results, the end-user will enter the search terms it considers most relevant to his or her topic of interest. If the object of the search is to find out more information about a specific person, the end-user will typically enter that person's name as a search term. Once the search term has been entered, the provider of the search engine will provide a list of results which the provider deems might relevant for the user. If the search term was a name, the list of search results will typically include links to websites which include the name of the person that was used as a search query.

1003. DATA FLOWS – Arrow (2) depicts the information flow between end-users and search engine providers. The arrow is bi-directional as end-users can both disclose

---

results. Their use indicates that the publisher does not want certain information on the source web page to be retrieved for dissemination through search engines.")

[2073] In this regard, it is important to note that the Robots Exclusion Protocol is a de facto standard, which is not enforced by anybody and there are no guarantees that all web robots will abide by it. M. Koster, "A Standard for Robot Exclusion", not dated, available at http://www.robotstxt.org/orig.html (last accessed 12 January 2016).

[2074] For more information see Google, "Search engine optimization – Starter Guide", avaialable at http://static.googleusercontent.com/media/www.google.com/en//webmasters/docs/search-engine-optimization-starter-guide.pdf (last accessed 12 January 16)

[2075] J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 50.

[2076] *Id.*

[2077] *Id.*

[2078] *Id.*

personal data to search engine providers (through search terms) and collect personal from search engine providers (through search engine results and the accompanying "snippets").

2.4 INFRASTRUCTURE (SERVICE) PROVIDERS

1004. MAIN CHARACTERISTICS – Infrastructure (service) providers are the entities that operate the technical infrastructure which is necessary to support the interaction between web publishers, search engines and end-users. Examples include Internet Service Providers ("ISPs"), hosting service providers, device manufactures, the providers of operating systems, etc. While the role of these entities will not be discussed in detail, it is nevertheless worth noting their important role in supporting the dissemination and retrieval of information online.

3 ROLES

3.1 SEARCH ENGINE PROVIDER

1005. OUTLINE – In *Google Spain*, the Court of Justice was asked to assess the legal status of search engine providers under Directive 95/46. In light of the importance and relevance of *Google Spain* for the research question of this thesis, this section will present

(1) the question referred in *Google Spain*;

(2) the oral arguments of the parties in *Google Spain*;

(3) the 2008 Opinion by the Article 29 Working Party;

(4) the opinion of the Advocate-General in *Google Spain*; and

(5) the holding of the Court of Justice.

A. Question referred in Google Spain

1006. CONTROL OVER "THIRD-PARTY DATA" – In its request for a preliminary ruling[2079], the Spanish *Audencia Nacional* asked to Court of Justice to determine whether

> "*article 2(d) of Directive 95/46/EC [must] be interpreted as meaning that the undertaking managing the 'Google' search engine is to be regarded as the 'controller' of the personal data contained in the web pages that it indexes?"*

[2079] Judgement in *Google Spain* C-131/12, EU:C:2014:317.

For purposes of clarity, it should be noted that this question only concerned the processing undertaken by Google itself (i.e., the location, indexation, temporary storage and making available of third-party content).[2080] In other words, the question did not extend to the processing activities undertaken by website publishers, content providers and/or end-users of the search engines service.

B. Oral arguments[2081]

1007. ARGUMENTS BY GOOGLE – Google's counsel advanced several arguments as to why the search engine provider should not be considered as a "controller" within the meaning of article 2(d). To be considered a "controller", it was argued, it is first and foremost required that the entity concerned has the objective ("purpose") of processing personal data. Google's search engine, on the other hand, indexes websites "*indiscriminately*" (i.e., without targeting personal data per se). Therefore, the search engine provider cannot be considered to be acting as a "controller" for its processing of personal data contained on those websites.[2082] Instead, it is the publisher of the information who should be labelled as the sole controller of this data. After all, it was argued, Google's intervention is *purely accessory* in nature: it is merely making information published by others more readily accessible. If a publisher, for whatever reason, decided to remove certain information from its website, this information would (eventually) be removed from Google's index and no longer appear in its search results. As a result, Google's counsel continued, the role of a search engine should be thought of as that of an "intermediary" as described in articles 12-14 of the Directive 2000/31 or that of a telecommunications service provider as described in recital (47) of Directive 95/46.[2083]

1008. OPPOSING ARGUMENTS – Quite a different line of argumentation could be heard coming from the European Commission and the Member States. They emphasized the need to distinguish between the processing activities of publishers on the one hand, and the processing activities of search engines on the other hand. Search engines, it was

[2080] See questions 2.1 and 2.2 of the Reference for a preliminary ruling.

[2081] The account of the oral arguments presented here is based on personal notes made while attending the public hearing in *Google Spain*. It is not based on the written submissions of the parties to the Court of Justice.

[2082] A similar line of argument was also put forth in relation to question 2.1, which essentially asked whether Google's location, indexation, temporary storage and making available of personal data should be considered as processing within the meaning of article 2(b) of the Directive. See B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 12-13.

[2083] Recital (47) of Directive 95/46 states that "*Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service*".

argued, carry out many operations (collection of website content, storage, analysis, ranking, etc.) which are completely distinct from those carried out by the publisher of the information.[2084] For these operations, search engine providers exclusively determine both the purposes and the means.[2085] As a result, search engines should not be considered as mere "intermediaries", but rather as the providers of a value-added service for which they carry their own responsibilities.[2086] To strengthen the argument, it was asserted that the harm at issue mainly resulted from Google's activities: if the content at issue would not be (so readily) available through its search engine, the damage to the plaintiff's reputation would be considerably less.[2087]

C. Opinion of the Article 29 Working Party

1009. AMBIGUOUS APPROACH – In 2008, the Article 29 Working Party adopted an Opinion on data protection issues related to search engines. The Opinion addressed the role of search engine provider in relation to third-party data, albeit in somewhat cryptic terms. Specifically, the Working Party reasoned that

> "*The principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers. The formal, legal and practical control the search engine has over the personal data involve is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and*

[2084] See also Agencia Espanalo de Protección de Datos (Spanish Data Protection Agency), "Statement on Internet Search Engines", *l.c.*, p. 7 ("*Internet search engines carry out information processing of their own, distinct from that of the websites to which they facilitate access*".)

[2085] According to this view, Google's "purpose" is to list (references to) relevant website content in its search results with a view of generating revenue from advertising. Its "means" include the use of web crawlers, indexation techniques, caches, ranking algorithms, etc., all of which are controlled exclusively by Google.

[2086] It is worth noting that Google's opponents explicitly acknowledged that the search engine provider cannot be considered a controller for the initial act of publication (i.e. the uploading of content and/or subsequent display on the website). Rather, they argued that the collection, aggregation and dissemination of personal data undertaken by the search engine provider should be perceived as a distinct set of processing operations for which Google carries a responsibility independent from that of the publisher.

[2087] See also Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines", WP 148, 4 April 2008, p. 5 ("*Some search engines republish data in a so-called 'cache'. By retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate. The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive"*) (emphasis added).

> *search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases […]*".[2088]

This language appeared to help both sides in *Google Spain*: on the one hand, it offered support to Google's claim that it should not be considered a ("principal") controller of the personal data contained in the web pages that it indexes, at least in so far as it acts as an intermediary. On the other hand, the Opinion also offered support to the claim that a search engine does act as a controller towards its own processing operations, including indexation and the inclusion of content in its search results.

1010. PROPORTIONALITY TEST – Perhaps the most striking element of the Working Party's reasoning is its reference to the principle of proportionality. Instead of limiting itself to a mechanical application of the "controller" concept, the Article 29 Working Party used the principle of proportionality as a means to delineate the obligations of search engines under data protection law. In my opinion, the approach advanced by the Working Party may have resulted in the right outcome, but could have benefited from a more detailed discussion. In particular, Opinion 1/2008 failed to explain the relationship between the criteria set forth by article 2 (d) on the one hand, and the nature and scope of an entity's obligations under data protection law on the other hand. This point will be further developed later on.[2089]

D. Opinion of the Advocate-General

1011. PRELIMINARY OBSERVATIONS – The Opinion of Advocate General (AG) started by highlighting the many changes that have occurred since the enactment of Directive 95/46 and in particular "the emergence of the internet and the various related phenomena".[2090] Given this radical change in environment, the AG argued that one should avoid a "blind literal interpretation"[2091] of the controller concept. Instead,

> "*the principle of proportionality, the objectives of the Directive and the means provided therein for their attainment must be taken into account in order to achieve a balanced and reasonable outcome*".[2092]

[2088] Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines", *l.c.*, p. 14 (emphasis added).
[2089] See *infra*; nrs. 1065 et seq.
[2090] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 77. Search engines were still "*at their nascent stage*", he continued, and "*the provisions of the Directive simply do not take into account the fact that enormous masses of decentrally hosted electronic documents and files are accessible from anywhere on the globe and that their contents can be copied and analysed and disseminated by parties having no relation whatsoever to their authors or to those who have uploaded them onto a host server connected to the internet*." (*Ibid*, paragraph 78.)
[2091] *Ibid*, paragraph 81.
[2092] *Ibid*, paragraph 79.

1012. KNOWLEDGE AND INTENT – Having set forth his preliminary observations, the Advocate General argued that

> *"[T]he general scheme of the Directive, most language versions and the individual obligations it imposes on the controller are based on the idea of responsibility of the controller over the personal data processed in the sense that the controller is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing as personal data*."[2093]

It therefore followed, according to the AG, that the entity concerned must be "*aware of what kind of personal data he is processing and why*"[2094] in order to be considered a "controller". Specifically

> *"the data processing must appear to him as processing of personal data, that is 'information related to an identifiable person in some semantically relevant way and not a mere computer code."*[2095]

1013. NO CONTROL OVER THIRD-PARTY PAGES – Based on the foregoing considerations, the Advocate General concluded that search engines cannot be considered a "controller" of personal data on third-party source web pages. After all, he reasoned, a search engine provider

> "*is not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way*."[2096]

The AG further substantiated his argument by pointing to the fact that a search engine provider "*has no relationship with the content of third-party source web pages*", nor does it *"have any means of changing the information in the host servers*".[2097] He also pointed to recital (47) of the Directive, which stipulates that it is in principle the originator of a message (and not the provider of the communications service) which is to be considered as the controller of its content.[2098] Finally, the fact that search engine providers cannot "*in law or in fact*" fulfil the obligations of a controller in relation to the personal data on

---

[2093] *Ibid*, paragraph 82 (original emphases modified)
[2094] *Ibid*, paragraph 83.
[2095] *Ibid*, paragraph 83.
[2096] *Ibid*, paragraph 84.
[2097] *Ibid*, paragraph 86.
[2098] *Ibid*, paragraph 87. The AG continued by saying that "*[t]his recital, as well as the exceptions to liability provided by the eCommerce Directive 2000/31 [...] builds on the legal principle according to which automated, technical and passive relationships to electronically stored or transmitted content do not create control or liability over it*". (*Id*.) In this regard, it is worth observing that recital (47) also considers that the providers of telecommunications and electronic mails services "*will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service*".

source web pages, mandated the conclusion that a search engine provider cannot be considered as a controller in this regard.[2099]

1014. CONTROL OVER THE INDEX – The foregoing observations made by the Advocate-General seemed mainly to support the position of Google, at least in relation to their crawling activities. The index of a search engine, however, is a different matter. The Advocate General was quite resolute in his affirmation that search engine providers do "control" their indexes, which link key words to the relevant URL addresses.[2100] This conclusion was warranted because

> "*[t]he service provider determines how the index is structured and may technically block certain search results [...] [and] decides whether exclusion codes on source web are to be complied with or not.*"[2101]

The Advocate General thus appeared to be of the opinion that the structuring and population of a search engine index does involve processing of personal data "in a semantically relevant way".[2102] The outcome of this approach is that search engine providers are not considered controllers with respect to their initial collection and use of personal data (i.e. "for the purposes of crawling, analysing and indexing"[2103]), but are considered controllers in relation to their index once it is established.[2104]

1015. ASSESSMENT – While the distinction made by the Advocate General seems logical at first, it is also a bit artificial.[2105] After all, Directive 95/46 arguably intended to cover all stages of the data processing life cycle, from its initial collection through to its eventual deletion (see article 2(b)). By differentiating between the moment of collection and the later use of this data, the Advocate General appears to place the initial processing activities of search engines outside of data protection law.[2106] Be that as it

---

[2099] *Ibid*, paragraph 89-90. According to the AG, this absence of control also extends to data contained in the cache memory of an internet search engine ("*because the cache is the result of completely technical and automated processes producing a mirror image of the text data of the crawled web pages*") - except where the search engine provider decided not to comply with the exclusion codes. (*Ibid*, paragraph 92-93.)

[2100] *Ibid*, paragraph 91.

[2101] *Id.*

[2102] *Ibid*, paragraph 83.

[2103] *Ibid*, paragraph 84.

[2104] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 17-18.

[2105] By using a similar line of reasoning, one could also argue that someone who sends out a drone mounted with a video camera to canvas certain areas or conducts an analysis of internet traffic should not be considered a controller for the data he collects (seeing as much of the collected data may be of a non-personal nature) until he actually watches (or otherwise analyses) this data and determines that personal data was in fact recorded.

[2106] The conclusion of the AG on this point appears to have been fuelled mainly by pragmatic considerations. For example, how can a controller provide a data subject with (prior) information in accordance with article 10 or 11 if it does not yet know which data subjects it is dealing with? How can it ascertain accuracy? How can it ensure proportionality? Of course, nobody can be obliged to do the impossible (*impossibilium nulla est obligatio*). A more relevant question, however, is whether data controller obligations must indeed be interpreted in such a way that they actually prohibit data collection in situations where personal data cannot be readily identified as such in advance. This issue will be investigated later on (cf. *infra*; nrs. 1065 et seq).

may, the Advocate General embraced the premise that the providers of search engine services carry out a distinct set of processing operations for which they carry their own data protection responsibilities. While one can disagree as to the precise moment at which these providers may be considered "in control" of the processing of personal data, the basic premise still stands.[2107]

E. Holding of the Court of Justice

1016. PURPOSES AND MEANS – In relation to the activities of locating information on the internet, indexing it automatically, storing it temporarily and making it available to internet users, the Court of Justice embraced the arguments put forward by the European Commission and the Member States. The Court considered that:

> "*It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).*"[2108]

1017. SEPARATE ACTIVITIES – The Court of Justice also recognized that the processing activities of search engines should be distinguished from those carried out by the publishers of websites.[2109]

> "*the processing of personal data carried out in the context of the activity of a search engine can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page.*"

1018. PRIVACY IMPACT – Finally, the Court of Justice also explicitly considered the impact of search engine services upon individual's privacy, acknowledging that search engines play a decisive role in the overall dissemination of information online:

> "*[I]t is undisputed that that activity of search engines plays a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.*
>
> *Also, the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the*

[2107] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 18-19.
[2108] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 33.
[2109] *Ibid*, paragraph 35.

internet enabling them to establish a more or less detailed profile of the data subject.

Inasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved." [2110]

3.2 WEBSITE PUBLISHERS AND CONTENT PROVIDERS

1019. WEBSITE PUBLISHER – The act of loading content on a publically accessible webpage constitutes "processing" of personal data within the meaning of article 2(b).[2111] In cases where the content has been authored or selected by the website publisher, the publisher shall in principle be deemed a controller in relation to this processing activity.[2112] The scope of control of the website publisher in principle extends to (1) the decision to include personal data on website; (2) the decision to render personal data accessible via the internet and (3) allowing indexation by search engines (unless robots.txt is used in such a way to indicate wish not to be indexed).[2113] In cases where the content was not authored or selected by the website publisher, but instead stored at the request of the recipient of the service, the legal status of the website publisher is similar to that of the OSN provider in relation to third-party data.[2114]

1020. CONTENT PROVIDER – Individuals posting content on a website shall in principle also be considered as controllers within the meaning of article 2(d) of Directive 95/46 (unless they are acting on behalf of or under the authority of someone else).[2115]

[2110] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 36-38. See also paragraph 34 ("*Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.*").

[2111] See also Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paragraph 25.

[2112] See also Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 40 ("*It follows from the above findings in Lindqvist that the publisher of source web pages containing personal data is a controller of processing of personal data within the meaning of the Directive. As such the publisher is bound by all the obligations the Directive imposes on the controllers.*")

[2113] See also Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 41-42.

[2114] Cf. *supra*; nrs. 813 et seq.

[2115] See also *supra*; nr. 819.

3.3 END-USER

1021. OPINION AG – Few commentators have explicitly reflected upon the legal status of the end-users of search engines. Although the Court of Justice was not asked to assess the legal status of end-users, the AG nevertheless indirectly reflected upon this issue as follows:

> "*Let us think of a European law professor who has downloaded, from the Court's website, the essential case-law of the Court to his laptop computer. In terms of the Directive, the professor could be considered to be a 'controller' of personal data originating from a third party. The professor has files containing personal data that are processed automatically for search and consultation within the context of activities that are not purely personal or household related.*"[2116]

1022. PURPOSES AND MEANS – The example cited by the AG was mainly intended to caution the Court against an overly broad interpretation of the Directive. Strictly speaking, however, the end-user does determine his own "purposes and means" when processing personal data by means of a search engine. As a result, end-users of search engines can be considered as controllers in relation to their own processing activities, namely (1) the entering of search terms containing personal data and (2) any further processing of personal data obtained through search results.

1023. PERSONAL USE EXEMPTION – Individuals who make use of internet search engines in a purely personal capacity shall in principle be exempted from compliance in accordance with article 3(2) of Directive 95/46.[2117]

1024. ASSESSMENT – Many would agree with the AG that applying Directive 95/46 to the end-users of search engines, even when they act outside of a context which is purely personal or household related, may lead to excessive and unreasonable legal consequences.[2118] On the other hand, few would disagree that a prospective employer that uses search engines to obtain more information about job applicants should be viewed as a controller in relation to his collection and subsequent processing of information. Whether or not the qualification of an entity as controller in fact leads to excessive and unreasonable consequences, depends mainly on the responsibilities and other consequences associated with this qualification. This issue will be revisited later on.[2119]

[2116] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 29.
[2117] Cf. *supra*; nrs. 868 et seq.
[2118] See e.g. House of Lords, European Union Committee, "EU Data Protection Law: A 'right to be forgotten'?", HL Paper 40, London, The Stationairy Office Limited, 30 July 2014, at paragraph 41.
[2119] Cf. *infra*; nrs. 1132 et seq.

3.4 *INFRASTRUCTURE (SERVICE) PROVIDERS*

1025. ISPs AND HOSTS – Infrastructure service providers, such as Internet Service Providers ("ISPs") and hosting service providers, act as controllers in relation to the processing of personal data they undertake in order to provide their services. The scope of control exercised by these entities in principle only extends to the processing of additional personal data (e.g., traffic data) necessary for the operation of the service and not to content stored on their servers or transmitted through their networks.[2120]

4 ALLOCATION OF RESPONSIBILITY AND RISK

1026. OUTLINE – The previous section concluded that each of the actors identified in section 2 can be considered as a "controller" within the meaning of Directive 95/46, at least in relation to certain processing operations. This section will elaborate upon the legal implications of this conclusion.[2121] Rather than discuss the obligations of each entity separately, the analysis will be structured according to data protection requirements. For each requirement, it will then be analysed how the obligations of each actor are currently interpreted. This approach will allow for a better evaluation regarding the extent to which the current allocation of responsibility and risk promotes effective implementation of data protection requirements. It will also enable reflection as to whether or not Directive 95/46 enables the taking into account of other basic principles of EU law, such as the principle of proportionality.

4.1 *LEGITIMACY*

1027. SEARCH ENGINE PROVIDER – Search engines can in principle legitimate their processing of third-party data on the basis of article 7(f). In his Opinion in *Google Spain*, the Advocate General identified three separate legitimate interests justifying the provision of search engine services:

> *"(i) making information more easily accessible for internet users;*
>
> *(ii) rendering dissemination of the information uploaded on the internet more effective; and*

[2120] See Recital (47) of Directive 95/46/EC.

[2121] As noted above, this analysis only concerns the allocation of responsibility and risk in relation to the processing personal data included on websites. It does not pertain to the data protection obligations which search engines have in relation to their users (in their capacity as users).

(iii) enabling various information society services supplied by the internet search engine service provider that are ancillary to the search engine, such as the provision of keyword advertising."[2122]

1028. BALANCE OF INTERESTS – Article 7(f) only legitimates the processing of personal data for as long as the interests served "*are not overridden by the interests or fundamental rights and freedoms of the data subject*". It is worth noting that article 7(f) also refers to the legitimate interests of third parties. Hence, the interests of search engine users – specifically their right to freedom of expression and information – may also be taken into account when considering the legitimacy of processing.[2123]

1029. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers may have various legitimate reasons for posting personal data online. In his opinion, the AG noted that web publication "*is a means for individuals to participate in debate or disseminate their own content or content uploaded by others on internet*".[2124] Website publishers and content providers can therefore in principle also legitimate their processing activities on the basis of article 7(f), provided also that the interests served are not overridden by the interests or fundamental rights and freedoms of the data subject.[2125] Depending on the circumstances, web publishers and content providers might also be to invoke other grounds of article 7 of Directive 95/46, such as data subject consent.

1030. END-USERS – Internet users have the right to seek and receive information made available on the internet, both by consulting the source web pages or by using internet search engines.[2126] The processing of personal data undertaken by end-users when using a search engine may therefore also, as a matter of principle, be justified on the basis of article 7(f) (unless the search results are used in manner which constitutes an

---

[2122] Each of these legitimate interests correspond to three fundamental rights protected in the Charter: freedom of information and freedom of expression (both in Article 11) and freedom to conduct a business (Article 16). See Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 95. During oral arguments, the counsel for the European Commission also explicitly confirmed that the providing of a search engine service can be considered a legitimate interest within the meaning of article 7(f). See also Spanish Data Protection Agency (AEPD), "Statement on Internet Search Engines", *l.c.*, 6.

[2123] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 30. See also *infra*; nr. 1049.

[2124] Opinion of Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 122.

[2125] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 30. In this regard, the Court of Justice noted that the ground justifying the publication of a piece of personal data on a website does not necessarily coincide with that which is applicable to the activity of search engines. Moreover, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page. (Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 86.)

[2126] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 121.

excessive interference with the interests, rights or fundamental freedoms of the individual concerned).

4.2 PRINCIPLES OF DATA QUALITY

A. Purpose specification and use limitation

1031. SEARCH ENGINE PROVIDER – The purpose specification principle implies that search engines may only index personal data for pre-defined purposes. The stated purpose of Google is "*to organize the world's information and make it universally accessible and useful*".[2127] In other words, the primary purpose of the search engine provider is to deliver the search engine service, at least as far as its processing of third-party data is concerned.

1032. WEB PUBLISHER AND CONTENT PROVIDER – Web publishers and content providers must also have a specific and legitimate purpose for making information available online. There are many such purposes imaginable: provisioning of information, news reporting, literary expression, etc. Regardless of the actual purposes pursued by a web publisher or content provider, the act of dissemination will generally constitute an exercise of his or her right to freedom of expression.[2128] In case of processing for "journalistic, literary or artistic" purposes, the content provider and/or web publisher may benefit from the exemptions or derogations established pursuant to article 9 of Directive 95/46.[2129]

1033. END-USER – End-users may pursue various objectives when using internet search engines. As indicated earlier, search queries performed by end-users can generally be categorized into three broad categories, namely "informational", "navigational" and "transactional".[2130] The specific purpose for which an end-user makes use of a search engine may vary from one search query to another.

B. Proportionality

1034. SEARCH ENGINE PROVIDER – In his Opinion in *Google Spain*, the AG dealt rather succinctly with the principles of data quality. In his view, the index of a search engine complies with the criteria of adequacy, relevancy and proportionality "*inasmuch as [...] the data corresponding to the search term really appears or has appeared on the linked*

[2127] Google, "Google's mission is to organize the world's information and make it universally accessible and useful", Google Company, not dated, available at https://www.google.com/about/company/ (last accessed 13 January 2016).
[2128] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 32.
[2129] See also *infra*; nr. 1050.
[2130] J. Van Hoboken, *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, *o.c.*, p. 50.

web pages […]".[2131] In other words: as long as the data corresponding to the search term really appears or has appeared on the linked web pages, article 6(1)c is complied with. As to the requirement that personal data should not be stored longer than necessary (article 6(1)e), the Advocate-General was similarly succinct. He merely stated that this requirement should (also) be assessed "*from the point of view of the processing in question, that is provision of information location service, and not as an issue relating to the content of the source web pages.*"[2132]

1035. ASSESSMENT – Although brief, the reasoning of the Opinion of the Advocate General underlines an important point: controller obligations must be evaluated in light of the scope of their "control" as well as the purposes pursued by the processing. Given the stated purpose of search engines (to help make online information more easily accessible), the AG argued that the requirements of relevancy and adequacy are met as long as data corresponding to the search term actually appears or has appeared on the linked web pages.[2133] The Opinion of the AG failed to consider, however, that the impact of the processing towards the individual concerned may be excessive in particular situation. Arguably, it would be unreasonable to require the search engine provider to assess the potential impact of every search result on proactive basis. Once the search engine is made aware, however, of the fact that the display of certain search results following a name search has a significant adverse impact on the privacy interests of the individuals concerned, the proportionality of processing must be reassessed.[2134]

1036. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers must assess the potential impact of making personal data publically available *prior* to loading it onto a public webpage. In principle, they should also reassess, from time to time, whether it is still necessary to keep the personal data online in light of the purposes pursued by the processing. If appropriate, the website publisher should remove or anonymize personal data if it is no longer necessary to keep the data online in identifiable form, or consider the use of the robots.txt exclusion protocol.[2135]

1037. END-USERS – As a rule, it is impossible for end-users to determine in advance whether the search results retrieved by consulting an internet search engine shall be

---

[2131] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 98.
[2132] *Id.* In the context of search engines, this seems to imply that (personal) data will have to be removed when the original data is removed as well (or when exclusion codes are put in place).
[2133] In the same vein: M. Peguera, "The Shaky Ground of the Right to Be Delisted", (Draft, August 2015), *l.c.*, p. 37-39.
[2134] See also *infra*; nr. 1049.
[2135] See also Tribunal Supremo. Sala de lo Civil, *A and B v Ediciones El Pais*, Judgment number 545/2015, ECLI:ES:TS:2015:4132. For a discussion see H. Tomlinson, "Case Law, Spain: A and B v Ediciones El Pais, Newspaper archive to be hidden from internet searches but no 're-writing of history'", *Inforrm's Blog*, 19 November 2015, accessible at https://inforrm.wordpress.com/2015/11/19/case-law-spain-a-and-b-v-ediciones-el-pais-newspaper-archive-to-be-hidden-from-internet-searches-but-no-re-writing-of-history-hugh-tomlinson-qc/ (last accessed 12 May 2016). See also Cour de Cassation, Arrêt C.15.0052.F, 29 April 2016 (upholding a decision of the Court of Appeal of Liège requiring the publisher of a newspaper to anonymise the litigious article online version of its digital archive).

"adequate, relevant and not excessive in relation to the purposes for which they are collected". Only once the results have been retrieved can the end-user actually determine whether this is the case. As a result, the end-user can effectively only comply with the principle of proportionality after collection (e.g., by limiting further storage or subsequent use of personal data which has been retrieved using a search engine).

1038. ASSESSMENT – The previous paragraphs illustrate that the principle of proportionality may impact different actors in different ways. Whereas website publishers and content providers are in principle obliged to assess the proportionality of disclosure *ex ante*, the provider of a general internet search engine can generally only be expected to assess proportionality ex post (once it has been made aware of the impact of its activities in a particular situation). These discrepancies result not only from the fact that each actor pursues different purposes, but also from the nature of their operations and the assessment of what constitutes a reasonable obligation "*within the framework of its responsibilities, powers and capabilities*".[2136]

C. Accuracy

1039. SEARCH ENGINE PROVIDER – Every controller is obliged to take "every reasonable step" to ensure the accuracy of personal data under its control.[2137] During oral arguments in *Google Spain*, the counsel for the European Commission indicated that search engines generally cannot be expected to (proactively) verify the accuracy of the information they reference.[2138] Given the volume of personal data processed by internet search engines, as well as the purposes they pursue, it would indeed be unreasonable to require search engines to establish the accuracy of personal data prior to including it in their index or search results.[2139] It is reasonable, however, to require search engines to assess the accuracy of information reactively (e.g., upon notification of its inaccuracy). Even though a search engine is not directly responsible for the accuracy of third-party content as such, its continued referral to inaccurate after notification may be excessive.

[2136] See also *infra*; nrs. 1065 et seq.

[2137] Article 6(1)d of Directive 95/46.

[2138] In his Opinion, the Advocate General went even further in stating that the personal data contained in Google's index or cache cannot be regarded as incomplete or inaccurate. (Opinion of Advocate General Jääskinen, *Case C-131/12*, paragraph 105.) The conclusion advanced by the Advocate General builds upon his earlier assessment that the principles of data quality may be deemed satisfied as long as the search term really appears or has appeared on the linked web pages. This interpretation is at odds with an earlier Opinion of another Advocate General, namely the Opinion drawn up by the Advocate General Kokkot in the *Satamedia* case. In this case, the Advocate General specified that "further processing of personal information which is proved to be false cannot be justified by the fact that it has been published" (Opinion of Advocate-General Kokott in *Satamedia*, Case C‑73/07, EU:C:2008:266, paragraph 124.) Even though the personal data is publicly available already, the data subject will still maintain a right to prevent the "*perpetuation and intensification of interference by means of the further processing of information, for instance, in the case of erroneous information [...]*." (*Ibid*, paragraph 122)

[2139] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 36.

1040. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers must take every reasonable step to ensure the accuracy of personal data prior to uploading it to a publically available webpage. They must also take every reasonable to keep personal data up to date and to ensure that inaccurate data are rectified.

1041. END-USERS – End-users cannot determine the accuracy of personal data retrieved through search results in advance. Only once the results have been retrieved can the end-user actually determine whether this is the case. As a result, the end-user can effectively only comply with the principle of accuracy after collection (e.g., by consulting additional sources and rectifying local copies of retrieved data as needed).

1042. ASSESSMENT – The principle of data accuracy, similarly to the principle of proportionality, may impact different actors in different ways. Which measures may be considered as "reasonable" will vary in light of the purposes pursued by the processing and the powers and capabilities of each actor.

4.3 TRANSPARENCY

1043. SEARCH ENGINE PROVIDER – The collection of third-party data by search engines is by definition indirect. Article 11(1) of Directive 95/46 specifies that in case of indirect collection, the data subject should in principle be provided with information regarding at least the identity of the controller and the purposes of the processing. Article 11(2) adds, however, that the controller shall not be obliged to inform the data subject if the provision of such information proves impossible or would involve a disproportionate effort. Given the scale of their operations and the purposes pursued, it can be argued that actively notifying each data subject of every collection constitutes a disproportionate effort.[2140]

1044. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers may collect personal data either directly from the data subject or indirectly. In case of direct collection, the data subject must in principle be informed of at least the identity of the controller and the purposes of the processing (except where he already has this information or if another derogation or exemption applies).[2141] If it is envisaged that personal data shall be made available online, the data subject should in principle also be informed thereof.[2142]

[2140] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 37.

[2141] E.g., in case of processing for journalistic, artistic or literary purposes.

[2142] In case of indirect collection, the website publisher is not obliged to inform the data subject when the provisioning of information proves impossible or would involve a disproportionate effort. In addition, website publishers may be exempted from the obligation to inform data subject pursuant to the journalistic exemption of article 9 (which permits exceptions for both direct and indirect collection).

1045. END-USERS – The collection of third-party data by end-users is by definition also indirect. End-users shall typically also be exempted from notice obligation, though there may be situations where it arguably would not require disproportionate effort for end-users to inform the individual concerned (e.g., during a recruitment process, if information collected through search engines is used to assess a job applicant).

4.4 CONFIDENTIALITY AND SECURITY

1046. SEARCH ENGINE PROVIDER – As the processing of third-party data is concerned, it seems that the obligation to ensure confidentiality and security of processing (articles 16 and 17 of Directive 95/46) holds only limited meaning for search engines. After all, third-party data processed by internet search engines will – by definition – already be publicly available (otherwise it would not be indexed by the search engine).[2143] The main obligation for search engines in this respect is to ensure the integrity of personal data contained in its index (i.e. guard against unauthorized alterations).[2144]

1047. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers should implement appropriate technical and organisational security measures to ensure the confidentiality and security of personal data which is placed online but is not authorized for public disclosure. Even if the information is intended to be accessible the public, it may nevertheless be appropriate in certain cases to take appropriate measures to limit indexing by search engines (e.g., a website operated by a public authority which publishes a list of recipients of agricultural subsidies).

1048. END-USERS – End-users in principle do not need to implement any measures to ensure the confidentiality and security of personal data collected through search engines, unless the data is subsequently brought in combination with other (non-public) personal data.

4.5 RIGHT TO OBJECT AND TO ERASURE

1049. SEARCH ENGINE PROVIDER – In *Google Spain*, the Court of Justice recognized that the provider of a search engine must, as a matter of principle, accommodate the data subject's rights to object and to erasure.[2145] Specifically, the Court held that –

[2143] Consequently, a duty of confidentiality understood as a prohibition of unauthorized disclosure or access seems nonsensical in a search engine context, because it can be assumed that data that is placed online (without putting in place exclusion codes or other tools to obscure data) is intended for viewing by an indefinite audience). (B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 38.)

[2144] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 38.

[2145] For a discussion of the rights of access and rectification see B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 38-41.

insofar as the conditions to exercise these rights are in fact satisfied – the operator of a search engine is obliged

> "*to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person*".[2146]

The data subject's "right to be delisted" applies only to search results that show up following a name search. The search engine provider must in principle accommodate a request for delisting unless there is a preponderant interest on the part of the general public in having access to the information in question by way of a name search.[2147] It is not required that the data are erased simultaneously or beforehand from the source web page, nor that the publication of the data on the source webpage is unlawful.[2148]

1050. WEBSITE PUBLISHERS AND CONTENT PROVIDERS – Website publishers and content providers must also, as a matter of principle, accommodate the data subject's right to object and to erasure. It should be noted, however, that the assessment may result in a different outcome:

> "*[N]ot only does the ground, under Article 7 of Directive 95/46, justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing of the interests at issue to be carried out under Article 7(f) and subparagraph (a) of the first paragraph of Article 14 of the directive may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same.*"[2149]

[2146] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 88.

[2147] *Ibid*, paragraph 97-99. Relevant criteria include the nature of the information in question, its sensitivity for the data subject's private life and on the interest of the public in having unbridled access to that information (an interest which may vary, in particular, according to the role played by the data subject in public life). (*Ibid* paragraph 81.) For a further elaboration of the criteria to be considered by search engine operators implementing *Google Spain* see Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12", WP 225, 26 November 2014, p. 12-20; X., "The Advisory Council to Google on the Right to be Forgotten", 6 February 2015, p. 7-14, available at https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view (last accessed 13 January 2016) and J. Ausloos and A. Kuczerawy, "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain ruling", *CiTiP Working Paper Series*. 5 October 2015, p. 27-37, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2669471 (last accessed 14 January 2016).

[2148] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 81.

[2149] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 86. The Court of Justice continued as follows: "*Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more*

Moreover, the processing of personal data by the publisher of webpage may, in some circumstances be carried out "solely for journalistic purposes" and thus benefit from an exemption by virtue of Article 9 of Directive 95/46.[2150] As a result, it cannot be ruled out that in certain circumstances the data subject may be capable of exercising his right to object and to erasure against that operator but not against the publisher of the web page.[2151]

1051. END-USERS – End-users who are not covered by the exemption for purely personal or household activities, or any other derogation or exemption, must in principle also accommodate data subjects' right to object and to erasure.

5 EVALUATION

1052. OUTLINE – The *Google Spain* decision may fairly be characterized as a milestone in European data protection law. In addition to settling important issues of applicable law and data subject rights, it also dealt extensively with the core concepts of the Directive. The purpose of this section is to assess the interpretation put forward by the Court of Justice as well as its implications for other actors involved in the processing of personal data.

5.1 TRUE TO BOTH LETTER AND SPIRIT

1053. A LITERAL AND TELEOGICAL APPROACH – In his advisory opinion, the Advocate General cautioned against a "blind literal interpretation" of the controller concept. [2152] Too much had changed since the Data Protection Directive was enacted.[2153] A literal interpretation would render the Directive applicable to a wide range of situations unanticipated by the Community legislature. This, in turn, would lead to unreasonable and excessive legal consequences.[2154] At first glance, it appears as if the Court of Justice simply brushed aside these words of caution. It opted for a formal approach, sticking close to the literal wording of article 2(d). But the Court also invoked a teleological argument[2155]:

---

significant interference with the data subject's fundamental right to privacy than the publication on the web page." (*Ibid*, paragraph 87).

[2150] *Ibid*, paragraph 85.

[2151] *Id.*

[2152] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 81.

[2153] *Ibid*, paragraph 77.

[2154] *Ibid*, paragraph 30.

[2155] See also G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law* 2014, Vol. 21, No. 3, p. 568; O. Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez", *The Modern Law Review* 2015, Vol. 78, no. 3, p. 524 ("*Resorting to both a literal and teleological interpretation of the Directive, the Court held that a search engine should not be excluded from the definition*

> "*it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.*"[2156]

Later on in its reasoning, the Court of Justice expanded at some length to consider the impact of internet search engines on individuals' privacy. Specifically, it noted that search engines render personal data accessible to internet users "*who otherwise would not have found the web page on which those data are published*".[2157] The Court also noted that *"the organisation and aggregation of information […] effected by search engines […] may, when users carry out their search on the basis of an individual's name, result in […] a more or less detailed profile of the data subject."*[2158] The reasoning of the Court of Justice recalls two of the main privacy concerns associated with internet search engines, namely the decline of "practical obscurity" and "aggregation".

1054. PRACTICAL OBSCURITY – Practical obscurity exists where information is technically available, but can only be found by spending a considerable amount of time and effort.[2159] Such would be the fate of most online information were it not for search engines. Search engines make it easy to locate information which would otherwise, from a practical perspective, be too difficult to locate. Ordinarily speaking, this is precisely the added value of search engines. But when the search target is a private individual, the efficiency gains offered by search engines may entail a privacy cost.[2160]

---

of controller and, in this way, the Court preserved the broad personal scope of application of the Directive.") and D. Sancho-Villa, "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten", *Legal Issues of Economic Integration* 2015, Vol. 42, no. 4, p. 369 (arguing that the Court of Justice relied primarily on a teleological interpretation rather than a formal analysis).

[2156] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 34.

[2157] *Ibid*, paragraphs 36-37.

[2158] *Ibid*, paragraphs 36-37.

[2159] See W. Hartzog and F. Stutzman, "The Case for Online Obscurity", *California Law Review* 2013, Vol. 101, No. 1, p. 21. Hartzog and Stutzman attribute term "practical obscurity" to the 1989 U.S. Supreme Court judgment *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* [489 U.S. 749 (1989)]. In this case the Supreme Court recognized that individuals have a privacy interest in maintaining the practical obscurity of so-called "rap sheets". Rap sheets are aggregated criminal records compiled by the FBI on the basis of state and local records. Even though the underlying information is ostensibly part of "the public record" (each item can in principle be found after a diligent search of local courthouse files, county archives, etc.), the Supreme Court considered this information to be "practically obscure" (because of the extremely high cost and low likelihood of the information being compiled by the public). The difference between, on the one hand, distributed, decentralized and hard-to-locate information, and, on the other hand, a centralized computer file was considered significant enough to justify non-disclosure under article 7c of the Freedom of Information Act (which excludes from disclosure records or information compiled for law enforcement purposes which constitute an "unwarranted invasion of personal privacy").

[2160] See also See O. Tene, "What Google Knows: Privacy and Internet Search Engines", *l.c.*, p. 1441. Or, as Grimmelmann has put it: "*from a victim's perspective […] search works best when it works the least*" (J. Grimmelmann, "Speech engines", *Minnesota Law Review* 2014, Vol. 98, p. 907).

1055. AGGREGATION – The second privacy concern identified by the Court of Justice relates to what Solove has termed "aggregation".[2161] In the context of information privacy, *aggregation* refers to the gathering together of information about a person.[2162] While a single piece of information by itself may not be so revealing, several pieces combined together can be quite telling.[2163] As more and more life events are logged online (e.g., a high school graduation, a change in job, the participation in a charity drive, etc.), search engines are capable of collating increasingly detailed biographical pictures. If one carries out a search on the basis of an individual's name, the ensuing list of results may offer a (seemingly) comprehensive profile of the individual concerned. This profile may have a profound impact on a person's reputation, livelihood and personal development. Or, as the saying now goes: "*You are what Google says you are*."[2164]

1056. CHANGE OF CONTEXT – While the drafters of Directive 95/46 may not have envisaged the Web as we know it today, they were mindful of the privacy concerns highlighted by the Court of Justice. In fact, similar concerns had triggered the enactment of the very first EU data protection laws back in the 1970's.[2165] In this sense, the Court's ruling is true to both the letter and spirit of EU data protection law. At the same time, one should not lose sight of the context in which the Data Protection Directive emerged. Even if its concepts and principles are, for the most part, "technology neutral", the Directive was still enacted within a particular socio-technical context. This context was composed of implicit assumptions about technology and how it will be used.[2166] In other words: while being true to the values pursued by the Community legislature, the Court of Justice arguably applied them to a context unanticipated at the time of enactment.

[2161] D. Solove, "A taxonomy of privacy", *University of Pennsylvania Law Review* 2006, Vol. 154, No. 3, p. 506. See also O. Tene, What Google Knows: Privacy and Internet Search Engines", *l.c.*, p. 1458.

[2162] D. Solove, "A taxonomy of privacy", *l.c.*, p. 506.

[2163] *Id.*

[2164] M. Angelo, "You Are What Google Says You Are", Wired 11 February 2009, http://www.wired.com/2009/02/you-are-what-go. See also Meg Leta Ambrose, "You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship", *International Review of Information Ethics* 2012, Vol. 17, electronic copy available at: http://ssrn.com/abstract=2154353 (pointing out that much online information is in fact more ephemeral than commonly portrayed).

[2165] See e.g. A.R. Miller, "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society", *Michigan Law Review* 1969, vol. 67, p. 1105 And F. W. Hondius, *Emerging data protection in Europe*, *o.c.*, p. 101. See also V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 222; C.J. Bennet, *Regulating privacy. Data Protection and Public Policy in Europe and the United States*, *o.c.*, p. 14; L.A. Bygrave, *Data Protection Law. Approaching its Rationale, Logic and Limits*, *o.c.*, p. 97-98.

[2166] See M. Birnhack, "Reverse Engineering Information Privacy Law", *Yale Journal of Law and Technology* 2012, Vol. 24, , p. 68 et seq. and C. Reed, "The Law of Unintended Consequences - Embedded Business Models in IT Regulation", *l.c.*, paragraph 36 et seq.

5.2 *ABSENCE OF KNOWLEDGE OR INTENT*

1057. ISSUE AT STAKE – In his Opinion, the Advocate General argued that in order to be considered a controller, the entity concerned should at least be aware of the fact that he is processing personal data.[2167] Moreover, the entity should process the data "*with some intention which relates to their processing as personal data*."[2168] The Court of Justice implicitly rejected this argument, however, when interpreting the definition of "processing" contained in article 2(b) of the Directive. Specifically, the Court considered that it does not matter that the provider of the search engine "*also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data*".[2169] As a result, a search engine provider can be considered a "controller" even if he does not deliberately target personal data as such.[2170]

1058. IMPLICATIONS – Sartor argues that the approach adopted by the Court of Justice may lead to an overly broad application of the controller concept:

> *"[I]f choosing to process a data set would entail being the controller for the processing of any personal data in that data set, then whoever is running any machine that processes data passing through the internet (for instance a router, pushing forward data towards their destination) would count as a [controller] of the personal data transmitted by that machine, and would be liable for letting through any personal data that should not have been made accessible. The same would hold for providers caching internet data, or hosting them in the cloud."*[2171]

1059. ASSESSMENT – The argument advanced by Sartor is essentially a "slippery slope" argument. If knowledge or intent are not required to consider an entity a controller,

---

[2167] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 83. The mere "statistical fact" that web pages are likely to include personal data was deemed insufficient. (Ibid, paragraph 84).

[2168] *Ibid*, paragraph 82. See in the same vein also C. Mitchell-Rekrut, "Search engine liability under the Libe Data Regulation Proposal: interpreting third party responsibilities as informed by Google Spain", *Georgetown Journal of International Law* 2014, Vol. 45, p. 883-884 ("*It remains true that search engines do not "determine[] the purpose[] and means of the processing of personal data" as personal data. As the AG suggested, it would be improper to conflate a search engine's broad "purpose" of indiscriminately cataloguing content on the internet with the myriad individual purposes for which people and organisations throughout the world publish data on the internet as controllers."*) (original emphasis)

[2169] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 28 (" … *regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data."*).

[2170] In the same vein: P. De Hert and V. Papakonstantinou, "Comment – Google Spain -Addressing Critiques and Misunderstandings One Year Later", *Maastricht Journal of European and Comparative Law* 2015, Vol. 22, No. 4, p. 627 ("*'Knowledge' of the data controller or 'alteration' of the data, as Google contested, are not necessary conditions to this end."*). See also D. Sancho-Villa, "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten", *l.c.*, p. 371.

[2171] G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 570. (Note: in the original version of this article, the word "processor" appears instead of the word "controller" in the fourth line of the quote. As the remainder of the quote suggests, however, that the author in fact intended to use the word "controller". This has been confirmed separately with the author via email correspondence.)

every entity interacting with personal data might potentially be considered a controller, thereby exposing them to unwarranted liability risks. The risks would be particularly troublesome in cases where passive intermediaries are involved, such as the providers of mere conduit or hosting services. In my view, Sartor's argument omits two important considerations. Specifically, the argument fails to acknowledge that (a) different actors may be in control of different aspects of the processing, even when processing the same personal data[2172]; and (b) search engines do not merely transmit or store information at the request of the recipient of the service. Search engine services involve a distinct set of processing activities for which the search engine provider exclusively determines the purposes and means (see also *infra*).[2173]

1060. PURPOSE AS "FINALITY" – The reasoning of the Court of Justice lends further support for the proposition that the concept of "purpose" should be understood as "finality" rather than "interest".[2174] Even if the provider of a search engine has no personal interest in the content or outcome of a specific search query (other than providing the most relevant search results), it still determines the finality of the processing required to deliver the search engine service.

5.3 SHOOTING THE MESSENGER?

1061. SEARCH ENGINES AS INTERMEDIARIES – In *Google Spain*, Google portrayed itself as a "neutral intermediary" between content providers and content seekers. Search engines, it was argued, merely help individuals find content placed online by others. As a result, any harm suffered should be attributed directly to the content provider. Moreover, if one were to allow data subjects to exercise their rights towards search engines, this would shift the burden of compliance from the original content provider to the provider of the search engine service. It would, in other words, be the equivalent of "shooting the messenger".[2175]

1062. ACTIVE INVOLVEMENT – Google's opponents, on the other hand, claimed that the privacy harm suffered by the plaintiff is a direct result of the search engine service. They rejected the notion that Google acts as a "neutral intermediary", arguing that it actively

---

[2172] This is explicitly confirmed by recital (47) of Directive 95/46, as well as guidance by the Article 29 Working Party. See also *supra*; nr. 105.

[2173] See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 16; E. Defreyne and R. Romain, "L'arrêt « Google Spain » : commentaire et mise en perspective", *Revue du Droit des Technologies de l'Information* 2014, n° 56, p. 80-84; H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", *Maastricht Journal of European and Comparative Law* 2014, Vol. 21, No. 3, p. 558-559 and P. De Hert and P. Papakonstantinou, "Comment – Google Spain – Addressing Critiques and Misunderstandings One Year Later", l.c., p. 627.

[2174] Compare *supra*; nr. 959 et seq.

[2175] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 67.

directs the flow of information from one party to another.[2176] Moreover, the harm suffered by the plaintiff was a consequence, not so much of the initial publication, but rather of its remaining readily accessible through search engines. Without Google's intervention, it was argued, the publication in question would be far less likely to cause harm to the plaintiff's privacy interests.[2177]

1063. NEUTRAL OR BIASED? – The arguments made in *Google Spain* are similar to those often heard in discussions regarding the alleged "neutrality" of Internet search engines.[2178] Grimmelmann points out that there are two diametrically opposed theories regarding the nature of search engines.[2179] For some, a search engine ought to be viewed as a passive and neutral "conduit" between websites and users. For others, a search engine should be seen an active and opinionated "editor", who sifts through the internet and uses experts judgment to identify items of importance and interest.[2180] According to Grimmelmann, these two opposing theories "*form the rhetorical backdrop to the ongoing legal battles over search*".[2181] However, as Grimmelmann also points out, neither extreme is particularly satisfying. In practice search engines combine elements of both theories; acting both as conduits and editors at the same time.[2182]

1064. HYBRID ROLE OF SEARCH ENGINES – In *Google Spain*, the conflict concerned the crawling, indexing, storage and making available of personal data mentioned on a third-party web page. Given that the purposes and means of these processing operations are determined exclusively by the search engine itself, it seems only natural to qualify them as a "controller" for these activities. The difficulty lies, however, in separating those activities from the intermediary function performed by search engines. Some might argue that search engines act both as "content selectors" (i.e. "controllers") and "messengers" (i.e. "intermediaries") when making content accessible to end-users.[2183] In this light, it is difficult to maintain a strict separation between the "intermediary" function of search engines and the operations for which they act as "controllers". Any

---

[2176] See in the same vein also the statements by Chris Scott and Steve Wood before the House of Lords European Union Committee "*Google does not merely passively deliver information; Google sculpts the results.*" (Chris Scott) and "*[…] we did not agree with the analogy of a search engine as a mere conduit, if you like, of the information just passing through it. Given the level of interaction a search engine has and the interest it takes using algorithms when it is interacting with personal information and spidering the internet, we felt that the way in which the court advanced that issue was correct.*" (Steve Wood) (House of Lords, European Union Committee, "EU Data Protection Law: A 'right to be forgotten'?", *l.c.*, p. 13-14).

[2177] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 67.

[2178] For a critical analysis of the arguments regarding the "neutrality" of search engines and their role as "innocent messengers" see U. Kohl, "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)", *l.c.*, p. 4-11.

[2179] J. Grimmelmann, "Speech engines", *l.c.*, p. 871

[2180] Grimmelmann's own metaphor portrays search engines as "trusted advisors" in attempt to combine the best of both worlds (*Ibid*, p. 895 et seq.).

[2181] *Ibid*, 871.

[2182] *Ibid*, 873-874. See also B. Van Alsenoy, Kuczerawy, and Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 68.

[2183] A search engine's referencing (i.e. rendering accessible) of content is intrinsically linked to its indexation and analysis of such content: cf. *supra*; nrs. 991 et seq.

allocation of responsibility in relation to the latter activity will inevitably have implications upon the former. Whether or not one considers such allocation to be appropriate, however, may simply depend on one's perception as to which aspect of the search engine service is dominant (selection or messaging).[2184]

5.4 SCOPE OF OBLIGATIONS OF SEARCH ENGINE PROVIDERS

1065. PROBLEM STATEMENT – Critics of *Google Spain* argue that the Court of Justice was wrong in considering search engines as "controllers", because such a categorization has unreasonable consequences.[2185] Their argument is based, at least in part, on the premise that search engines are unable to comply with all of the obligations and restrictions that the Directive typically imposes upon controllers.[2186] A similar line of reasoning had also led the AG to conclude that search engines should not be considered as controllers in relation to the personal data on source web pages hosted on third-party servers.[2187]

1066. TAILORING OBLIGATIONS – Most of the provisions of Directive 95/46 allow for flexibility in their application. Several provisions have explicit "safety-valves" built in, which allow for derogations in cases where strict compliance would be disproportionate or unreasonable.[2188] For provisions that do not have such explicit safety-valves built in,

---

[2184] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 68. Compare also M. Peguera, "The Shaky Ground of the Right to Be Delisted", (Draft, August 2015), p. 31 et seq., available at http://ssrn.com/abstract=2641876 (last accessed 25 August 2015).

[2185] G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 570 and M. Peguera, "The Shaky Ground of the Right to Be Delisted", *l.c.*, p. 29-30).

[2186] See e.g. M. Peguera, "The Shaky Ground of the Right to Be Delisted", *l.c.*, p. 29: "*the question arises as to whether this characterization can be seen as a proportionate outcome in terms of the legal duties that stem from it. Considering search engines as controllers is not without consequences, as they are unable to comply with most of the obligations the Directive imposes on data controllers.*"

[2187] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 89-90 ("*In my view the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data on source web pages hosted on third-party servers. Therefore a reasonable interpretation of the Directive requires that the service provider is not generally considered as having that position. An opposite opinion would entail internet search engines being incompatible with EU law, a conclusion I would find absurd. Specifically, if internet search engine service providers were considered as controllers of the personal data on third-party source web pages and if on any of these pages there would be 'special categories of data' referred to in Article 8 of the Directive (e.g. personal data revealing political opinions or religious beliefs or data concerning the health or sex life of individuals), the activity of the internet search engine service provider would automatically become illegal, when the stringent conditions laid down in that article for the processing of such data were not met.*")

[2188] See also Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", WP 136, 20 June 2007, p. 4-5 ("*Even where processing of personal data within the scope of the Directive is involved, not all the rules contained therein may be applicable in the particular case. A number of provisions of the Directive contain a substantial degree of flexibility, so as to strike the appropriate balance between protection of the data subject's rights on the one side, and on the other side the legitimate interests of data controllers, third parties and the public interest which may be present*"")

practitioners can fall back on the general principle of proportionality, which is a basic principle of EU law.[2189] As the Court of Justice observed in *Lindqvist*:

> "*it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.*"[2190]

1067. "RESPONSIBILITIES, POWERS & CAPABILITIES" – In *Google Spain*, the Court of Justice took care to interpret Directive 95/46 in such a way that it would not unduly restrict the offering of search engine services. In qualifying search engine providers as controller, the Court also immediately indicated that there may be limits to the obligations of search engine providers:

> "*[…] the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that*

[2189] For more information regarding the principle of proportionality as a basic principle of EU law see F.G. Jacobs, "Recent Development in the Principle of Proportionality in European Community Law", in E. Ellis (ed.), *The Principle of Proportionality in the Laws of Europe*, 1999, Hart Publishing, Oxford, p. 1-22 and C. Kuner, "Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies", *Privacy & Security Law Report* 2008, Vol. 7, no. 44, p. 2.

[2190] Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paragraph 87. In this regard, it is worth drawing attention to attention to *Volker und Markus Schecke*, a case decided by the Court of Justice in 2010. This case concerned the publication of information about the beneficiaries of certain agricultural funds. Pursuant to the relevant EU Regulations, Member States were required to publish the names of the beneficiaries of such aid, as well as the amounts received by each beneficiary. Two beneficiaries challenged this publication, one of whom was a private person, whereas the other was a legal person. The Court of Justice agreed with the referring Court that the drafters of the Regulation at issue had, at least insofar as the publication concerned private persons, insufficiently balanced the interests at stake. Where the information concerned legal persons, however, the Court of Justice considered that the publication of such information was in fact proportionate. The Court of Justice went on to observe that "*Furthermore, the obligation on the competent national authorities to examine, before the data in question are published and for each legal person which is a beneficiary of [agricultural] aid, whether the name of that person identifies natural persons would impose on those authorities an unreasonable administrative burden*". (Judgement in *Volker und Markus Schecke*, Joined Cases C‑92/09 and C‑93/09, EU:C:2010:662, paragraph 87). This cursory consideration by the Court of Justice illustrates a very important point, namely that a controller's obligations need to be interpreted within reason. While the Court of Justice recognized that data relating to a legal person might also (indirectly) constitute personal data, it stated that it would be unreasonable to oblige public sector bodies to investigate this in each instance prior to publication. By analogy, one can argue that search engines cannot be expected to conduct this analysis prior to undertaking its automated collection ("crawling") of webpages. To hold otherwise would require search engine providers to conduct a manual review of each website intended for indexation. Taking into account the scale of search engine operations, the ratio of personal to non-personal data, as well as the purposes of the processing, such a burden would arguably be unreasonable. See also B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 29-30.

effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved."[2191]

By explicitly referring to the "powers and capabilities" of the search engine operator, the Court of Justice implicitly acknowledged that there may be practical limits to the ability of a search engine operator to meet all the obligations resulting from Directive 95/46.[2192] In particular, it can be argued that *Google Spain* does not oblige search engine providers to exercise preventative control over the information it disseminates.[2193] In fact, the reasoning of the Court of Justice suggests that the obligations of search engine providers concerning third-party data essentially only "reactive": only after the provider has been made aware of the fact that the display of specific search results following a name search adversely impacts the data subject, must the provider assess whether or not delisting is necessary.[2194]

1068. CRITIQUE – Peguera and Sartor have called into question the approach of the Court of Justice by offering two critiques. The first critique is that this approach does not comport with the language of the Directive.[2195] While Directive 95/46 does exempt controllers from fulfilling certain obligations which would require disproportionate efforts, it does not do so in all instances (most notably in relation to sensitive categories of data).[2196] The second critique is that the approach of the Court of Justice may easily lead to inconsistent outcomes and therefore give rise to legal uncertainty.[2197] Sartor eloquently summarizes as follows

"The very need to use broad principles or questionable distinctions to pre-empt apparently straightforward implications of the Court's approach should lead us to question that very approach, and to doubt that it provides a sustainable legal framework, which may adequately support legal practice."[2198]

[2191] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 38.

[2192] For a more narrow reading see M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *l.c.*, p. 26.

[2193] H. Hijmans, "Right to Have Links Removed - Evidence of Effective Data Protection", *l.c.*, p. 559 ("*For me, it is obvious that this judgment does not mean that a search engine provider should exercise preventive control over the information it disseminates, nor that it is in any other manner limited in its essential role of ensuring a free internet. In essence, the Court confirms that a search engine – which has as its core activity the processing of large amounts of data with potentially important consequences for the private life of individuals – cannot escape from responsibility for its activities.*")

[2194] See also Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, p. 6 ("*The ruling does not oblige search engines to permanently carry out that assessment in relation to all the information they process, but only when they have to respond to data subjects' requests for the exercise of their rights.*")

[2195] M. Peguera, "The Shaky Ground of the Right to Be Delisted", *l.c.*, p. 29.

[2196] *Ibid*, 30. It should be noted, however, that the general prohibition on processing personal data does not apply in case of explicit consent of the data subject or if the data the processing relates to data which have been manifestly made public by the data subject.

[2197] *Id.*

[2198] G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 575.

The critique of Peguera and Sartor should not be taken lightly. If "reasonable" interpretations de facto exempt controllers from complying with certain obligations, there is a risk of undermining the effectiveness of the data protection framework as a whole.[2199]

1069. ASSESSMENT – The precise scope of data protection obligations must always be assessed in context. A controller's obligations might indeed be lighter - or more onerous - depending on the purposes pursued by the processing and the risks for data subjects.[2200] The critiques of Peguera and Sartor illustrate that certain provisions of Directive 95/46 fail to provide adequate flexibility in all contexts. Such a finding does not, however, undermine the validity of the controller concept as such, but rather requires us to reconsider how to the obligations associated with that concept should be formulated. The formulation of the Court of Justice ("*within the framework of its responsibilities, powers and capabilities*") may be considered a useful addition in this respect, which possibly merits inclusion in the legal framework.[2201]

5.5 IMPACT ON FREEDOM OF EXPRESSION

1070. RISKS OF OVER-COMPLIANCE – In his Opinion in *Google Spain*, the AG argued that allowing data subjects to exercise their rights vis-à-vis search engines would negatively impact freedom of expression. Specifically, he reasoned that:

> "Such *'notice and take down procedures', if required by the Court, are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers*".[2202]

Over-compliance with removal requests poses a significant threat to freedom of expression online.[2203] This problem is not, however, limited to matters concerning data protection.[2204] While certain types of content can more readily be identified as "illegal"

[2199] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 44-45. During oral arguments in Google Spain, the Advocate General asked the Commission whether it thinks that there is such a thing as a "light version" of the controller concept. In other words, is it appropriate to qualify an entity as a "controller" if many of its basic responsibilities are interpreted in such a lenient way? The European Commission responded by saying that the search engine's obligations should be assessed on a case-by-case basis, and only in the context of specific requests (*Ibid*, p. 44).

[2200] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 44.

[2201] Cf. *infra*; nrs. 1230 et seq.

[2202] Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 133 (emphasis added).

[2203] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 69.

[2204] European Commission, First Report on the Application of Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21 November 2003; European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the

or "inappropriate", an evaluation will always be necessary. And as long as intermediaries face an immediate threat of liability, the most cautionary approach is to act upon any indication of illegality, without engaging in any balancing of rights.[2205]

1071. MITIGATION STRATEGIES – A number of measures could be devised to help mitigate the risk of over-compliance with delisting requests. For example, one might grant the search engine provider some leeway, by saying that it shall only be obliged to delist if it is sufficiently clear that the interests of the data subject outweigh the interests of others.[2206] It is beyond the scope of this thesis, however, to investigate this matter in greater depth. Further research is necessary to determine which measures may be best suited to mitigate risks of over-compliance.[2207]

Directive on electronic commerce (2000/31/EC), available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf; European Commission, Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11 January 2012 SEC(2011) 1641 final.

[2205] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 69. See also *supra*; nr. 877.

[2206] In the same vein: G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 572-574 and M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *l.c.*, p. 25 et seq.

[2207] For a discussion of possible measures see: J. Ausloos and A. Kuczerawy, "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain ruling", *l.c.*, p. 17-25.

PART V

RECOMMENDATIONS

Chapter 1 INTRODUCTION

1072. RESEARCH OBJECTIVES – In the final part of this thesis, the insights developed over the three preceding parts shall be used as a basis for policy recommendations. In particular, this Part aims to provide policy recommendations as to how the current allocation of responsibility and risk among actors involved in the processing of personal data might be modified in order to increase legal certainty while maintaining at least an equivalent level of data protection.

1073. METHODOLOGY – The policy recommendations shall be developed on the basis four analytical stages. First, the issues identified in Part IV shall be summarised and presented in a structured manner (typology of issues). Second, an inventory will be made of ways in which these issues might be remedied (typology of solutions). Third, an evaluation will be made of the extent to which the proposed remedies are capable of addressing each of the identified issues. The evaluation of possible solutions shall, for the most part, be based on the typology of issues. Each proposal will be evaluated on the basis of whether, and if so, to what extent, it is capable of addressing each of the identified issues.[2208] If multiple solutions have been proposed to remedy a particular issue, an internal comparison will be made. Finally, in the fourth phase, the approach adopted by the European legislature in the context of the GDPR will be compared with the outcome of the preceding evaluations. Where relevant, recommendations for possible further improvements will be made.

1074. RELEVANT SOURCES – The typology of issues will be developed by categorising the issues identified in Part IV and presenting them in a structured manner. The typology of solutions, on the other hand, will be developed on the basis of proposals put forward by various stakeholders (policymakers, regulators, industry, academia and civil society). The evaluation of possible solutions shall, for the most part, be based on the typology of issues. Each proposal will be evaluated on the basis of whether, and if so, to what extent, it is capable of addressing each of the identified issues. If multiple solutions have been proposed, an internal comparison will be made. Where appropriate, insights from the field of law and economics will be applied to assist the internal comparison of the proposed solutions.[2209]

[2208] In other words, the development of normative recommendations shall be based on the evaluation of possible solutions and their ability to address the identified issues, as opposed to on the basis of abstract principles. As will be seen, however, certain abstract principles (e.g., legal certainty, effective and complete protection) have been involved in the identification of issues. As the typology issues shall act as a positive assessment framework, the relevant principles shall be incorporated in the analysis.

[2209] In other words, the typology of issues shall serve as the positive assessment framework to evaluate the proposed solutions. No additional assessment criteria will be used to evaluate the proposed solutions. Only in the context of the internal comparison of possible solutions, shall the insights from the field of law and economics be applied in order to enhance the evaluation process.

1075. PERSPECTIVE – At the moment of writing, the legislative process which has led to the General Data Protection Regulation has just come to an end. The outcome of the legislative deliberations is therefore already known. However, in order understand and evaluate the choices made by the EU legislature, it is useful to present each of the options which the EU legislature might have considered (or considered but rejected). For this reason, the typology of issues and solutions will be presented from the perspective of someone who is considering ways in which Directive 95/46 might be improved. After assessing each proposal, reference will be made to the final approach taken by the European legislature in the GDPR. In Chapter 4, the perspective will shift and will present recommendations for possible changes to the GDPR in the future.

Chapter 2 TYPOLOGY OF ISSUES

1 INTRODUCTION

1076. PREFACE – Part IV of this thesis demonstrated that applying the concepts of controller and processor can be difficult in practice. Practitioners often disagree as to whether an entity should be considered a controller or processor, or struggle to make an unambiguous determination. The objective of this Chapter is to provide a structured overview of the main issues that emerge in practice. To this end, a typology of issues shall be developed which categorizes the issues identified in Part IV and presents them in a structured manner.

1077. CATEGORISATION – The typology of issues shall be structured according to four traditional methods of legal interpretation, namely: (1) grammatical; (2) teleological; (3) systemic; and (4) historical. The chosen methods were retained simply because they are the methods of legal interpretation that have been relied upon - either explicitly or implicitly - by scholars, regulators and courts when evaluating the use cases documented in Part IV.[2210] Applying this categorisation, the following typology of issues can be developed:

(1) *Grammatical issues*: issues that concern the words chosen to define the concepts of controller and processor;

(2) *Teleological issues*: issues that concern the policy objectives that underlie the allocation of responsibility and risk between controllers and processors;

(3) *Systemic issues*: issues that arise in light of the functions fulfilled by the controller and processor concepts within the regulatory scheme of Directive 95/46; and

(4) *Historical issues*: issues that arise when applying the regulatory framework of Directive 95/46 to situations which were not envisaged by the European legislature.

1078. RESEARCH ASSUMPTION – The development of a typology of issues according to traditional methods of legal interpretation is motivated by the assumption that conflicts

[2210] For an overview of methods of legal interpretation see L. Kestemont, *Methods for traditional legal research*, Reader Research Master in Law: Methods of Legal Research. KU Leuven - University of Tilburg (Leuven/Tilburg), 2015, 36 p. See also W. Brugger, "Legal Interpretation, Schools of Jurisprudence, and Anthropology: Some Remarks from a German Point of View", *American Journal of Comparative Law* 1994, Vol. 42, No. 2, p. 395-421 and N. MacCormick, "Argumentation and Interpretation in Law", *Ratio Juris* 1993, Vol. 6, No. 1, p. 16-29.

of interpretation, as well as interpretative guidelines provided by courts and regulators, can help to uncover the main issues at stake.

1079. METHODOLOGY – The typology of issues will be developed following an internal approach. Reference shall in first instance be made to the text of the law and the preparatory works accompanying Directive 95/46. Where appropriate, reference shall also be made to court decisions, regulatory guidance and doctrine which concern the application of the controller and processor concepts.

1080. LIMITATIONS – The utility of the exercise undertaken over the following sections is predicated on the assumption that the selection of use cases analysed in Part IV offers a sufficiently representative account of the main issues that arise when applying the controller and processor concepts in practice.[2211] In other words, there can be no pretense at exhaustivity. Be that as it may, the analysis of proposals put forward in the context of the review of Directive 95/46/EC (cf. *infra*; typology of solutions) indicates that the typology of issues presented here is rather comprehensive. While the issues documented here fail to offer a definitive normative framework on the basis of which proposals for legislative change should be accepted or discarded, they nevertheless provide a useful framework for an informed and structured evaluation of competing policy options.

2 GRAMMATICAL

1081. PREFACE – The first category of issues arises from the grammatical interpretation of the controller and processor concepts. The grammatical interpretation method consists of *isolating the essential words* used in a legal provision and *clarifying their meaning* by reference to either the literal meaning of the words or their meaning in common parlance.[2212] The analysis of use cases in Part IV has revealed that the criteria (i.e. "essential words") to determine whether a party is acting as a controller or processor may be subject to multiple interpretations. The aim of this section is to detail how the existing criteria can be understood in different ways and to clarify how this may affect the interpretation of the concepts of controller and processor.

2.1 "DETERMINES"

1082. DECISION-MAKING POWER – To "determine", according to the Article 29 Working Party, means to exert factual influence by exercising decision-making power.[2213] The notion of "decision-making power" can be understood in different ways. The first meaning is formal, or normative in nature, and refers to the decision-making

[2211] See also *supra*; nr. 658.
[2212] L. Kestemont, *Methods for traditional legal research*, *o.c.*, p. 7.
[2213] Opinion 1/2010, *l.c.*, p. 8-9

power of persons which are *authorized* to lead and manage an organisation's activities.[2214] The second meaning is descriptive, or non-normative in nature, and refers to *factual influence*.[2215]

1083. AUTHORITY TO DECIDE – Traditionally, the legal status of controller has been attached to a party's *authority to decide* about the processing, rather than its involvement in the processing itself. Previous iterations of the controller concept in fact contained an explicit reference to authority: both the definition of the 1980 OECD Guidelines and Convention 108 describe the controller as the entity that is "*competent to decide*" about the processing.[2216] In Opinion 1/2010, the Working Party still attached considerable importance to the notion of "competence". While recognizing the functional nature of the controller concept, the Working Party also tried to link the question of decision-making power to both formal criteria (explicit competences) and traditional roles (implicit competences) as much as possible.[2217]

1084. FACTUAL INFLUENCE – The apparent emphasis on authority (explicit and implicit competences) may be contrasted with the increasing emphasis on *factual influence* over the processing. Even in Opinion 1/2010, the Working Party repeatedly underlined the "functional nature" of controller concept, which aims to allocate responsibility where factual influence is. As a result, it would appear that the word "determine" is used to convey a dual meaning: it can refer both to the (implicit or explicit) authority to decide about the processing as well as the exercise of factual influence over the processing.

1085. ISSUE – The dual meaning ascribed to the notion of decision-making power can give rise to difficulties when applying the controller concept in practice. While the two meanings may coincide, in practice this is not necessarily the case. A discrepancy between the "authority to decide" about the processing of personal data and "factual influence" over the processing of personal data is particularly likely to occur in cases where those engaged in the processing exercise considerable influence in deciding how

---

[2214] In her 1995 thesis, Overkleeft-Verburg also identifies two distinct meanings of the concept of "decision-making power". One the one hand, it can be understood in the "operational" sense, referring to an exercise of decision-making power by subordinates who have been tasked with undertaking the processing of personal data. On the other hand, it can also be understood in the "managerial" sense, referring to the decision-making power of persons which are authorized to lead and manage an organisation's activities. Overkleeft-Verburg points out that the Dutch legislator used both meanings interchangeably during the preparation of the Dutch Data Protection Act of 1989. This implied that the concept of a "controller" could refer to a wide variety of entities: a natural or legal person, a public body, the management board of an institution, the head of an administrative department, branch directors, etc. The ambiguous nature of the term resulted in considerable legal uncertainty in practice. See M. Overkleeft-Verburg, *De Wet persoonsregistraties - norm, toepassing en evaluatie*, *o.c.*, p. 369 et seq.

[2215] Regarding the difference between "power" (as factual influence) and "authority" (as normative influence) see also M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *l.c.*, p. 11-12.

[2216] Cf. *supra*; nr. 364 and nr. 396.

[2217] Opinion 1/2010, *l.c.*, p. 9-10.

the processing shall be organised. The cloud computing use case analysed in Part IV clearly supports this proposition.[2218]

2.2 "PURPOSE"

1086. FINALITY VS. INTEREST – A controller determines the "purposes" of the processing. The notion of "purpose" can be understood in different ways. The first meaning is subjective, or personal in nature, and results from a personal project, business, or activity for which data processing is essential (*purpose as interest*).[2219] The second meaning is objective, or non-personal in nature, and refers to the aims or objectives pursued by the processing itself (*purpose as finality*).

1087. INTEREST – Traditionally, the controller has been conceived of as the "main beneficiary" of the processing: the data processing is carried out "on his behalf", "for his activities", or "*for his purposes*".[2220] As a result, the absence of a personal interest in the outcome of the processing is often invoked as an argument to disqualify a particular actor as controller. In the case of cloud computing, for example, several authors argue that the absence of interest in the outcome of the processing implies that cloud providers should generally be viewed as processors rather than as controllers.[2221] A similar argumentation was also put forward in the context of the Pan-European Proxy Service envisioned by STORK and STORK 2.0.[2222]

1088. FINALITY – The "purpose" of the processing can also be understood in an objective sense, i.e. without reference to the subjective interests of the parties involved in the processing. Establishing the purpose of the processing then involves an analysis of the *aims or objectives* of the processing itself. To determine the finality of processing, one might ask questions such as "*What is the objective or material end of the processing?*" "*What is the output of the processing and what is the envisioned use of this output?*"[2223] Authors who consider cloud providers as controllers typically emphasize the role of the provider in (pre)determining the material ends of the processing services they offer (e.g., a SaaS application designed for CRM).[2224]

[2218] Cf. *supra*; nrs. 964 et seq.
[2219] Based on J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 181.
[2220] Cf. *supra*; nr. 960.
[2221] Mantelero, A., "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *l.c.*, section 3.2 ("*[…] the cloud provider receives the information to be processed in the interest of the user*") and L. Determann, "Data Privacy in the Cloud—Myths and Facts", l.c., Myth 10 ("*[…] providers tend to offer a platform or software functionality as a service, without any interest, knowledge, or influence regarding data types and processing purposes*"). Cf. *supra*; 925.
[2222] Cf. *supra*; 763.
[2223] See also on J.A. Salom, "'A third party to whom data are disclosed': A third group among those processing data", *l.c.*, p. 181.
[2224] Cf. *supra*; nr. 927.

1089. INTERPLAY AND OVERLAP – The distinction between finality and interest can be difficult to make in practice. The main reason is that finality and interest often go hand in hand. If a party involved in the processing of personal also has an interest in the outcome processing, he or she will typically also be involved in deciding the finality of processing. This is logical, seeing as the pursuit of an interest will involve the use of functionalities (i.e., instruments which yield certain outputs) that actually advance the interests of the actor concerned. The end-user of a service which involves the processing of personal data will therefore almost invariably be considered as a controller. On the other hand, it is possible for an actor to be involved in determining the finality of processing without having a personal interest in the outcome processing as such. The Working Party's analysis of e-Government portals clearly supports this proposition.[2225]

1090. ISSUE – The distinction between finality and interest is relevant in situations where an entity does not have an interest in the outcome of the processing, but is nevertheless involved in determining the finality of processing. Practitioners who understand purpose as finality (rather than interest) are more likely to consider service providers as controllers (or joint controllers) insofar as they autonomously design their processing services with a specific use in mind (e.g., a purpose-built SaaS application). Conversely, practitioners who understand purpose as interest are less likely to do so.

2.3 "AND"

1091. CUMULATIVE REQUIREMENT – Article 2(d) of the Directive provides that the controller determines the purposes *and* means of the processing. The use of the word "and" implies the existence of a cumulative requirement: an actor must be involved in determining both the finality (purpose) and modalities (means) of the processing in order to be considered a controller.

1092. INTERPRETATION BY WP29 – In Opinion 1/2010, the Working Party took the position that decisions about the technical and organisational means of the processing can be delegated by the controller to the processor.[2226] Against this background, the Working Party considered that the technical and organisational means of the processing might even be determined exclusively by the data processor.[2227] Only in cases where the determination of means concerns the "essential means" of the processing, or if the actor is involved in the determination of purposes, shall the actor concerned be deemed a (joint) controller rather than processor. [2228]

[2225] Cf. *supra*; nr. 771.
[2226] Opinion 1/2010, *l.c.*, p. 15.
[2227] Opinion 1/2010, *l.c.*, p. 14. See in the same vein also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 61-62.
[2228] *Ibid*, p. 19.

1093. ISSUE – Van Eecke and Truyens point out that the Working Party's distinction between "essential" and "non-essential" means (see also *infra*) is at odds with the literal wording of article 2(d).[2229] Specifically, they argue that the approach of the Working Party reduces a dual legal requirement ("and") to a single requirement ("or"), by stating that it is sufficient for a party to determine either the purpose or the essential aspects of the means in order to qualify as a data controller.[2230]

1094. CAVEATS – In theory, one could derive two premises from the guidance provided by the Article 29 Working Party. The first premise is that it is possible for an actor to determine the "means" of the processing without being involved in the definition of the "purpose" of the processing. Conversely, the second premise is that it is possible for an actor to determine the "purpose" of the processing without being involved in the determination of "means". While both premises would be valid, conceptually speaking, a number of caveats must be made. The first caveat is that every choice of "means" can be viewed as involving a determination of *the purpose of those means*. Means are not chosen in the abstract, but rather with a view of achieving a certain outcome or functionality (i.e. as "means to an end").[2231] The second caveat is that a choice of means might be as simple as a decision to make use of a service provided by a third party. Even if the entity concerned does not have the power to influence how the service is organized, it can at a minimum decide whether or not to use the service. In this sense, a controller still effectively determines the means of the processing when he entrusts the processing of personal data to a particular service provider, even if the only choice that is made in relation to the modalities of the processing is simply to "take it or leave it".[2232]

1095. ASSESSMENT – One should take care not to lose sight of the specific context in which the Working Party provided its guidance regarding "essential" and "non-essential" means of the processing. The aim of the Working Party was to clarify situations in which a processor can no longer be considered a mere "processor" but must instead be considered a controller (or joint controller). In other words, the primary objective of the Working Party was to clarify the "tipping point" at which a service provider's involvement is such that it becomes justified to subject the service provider to the obligations and responsibilities ordinarily incumbent upon controllers. The Working Party's distinction between "essential" and "non-essential" means should therefore be

---

[2229] P. Van Eecke and M. Truyens, "Privacy and social networks", *l.c.*, p. 539.

[2230] *Id.*

[2231] In the same vein: T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 107 ("*[…] le sous-traitant détermine évidemment la finalité même d'utilisation de ses services. Ainsi par exemple, le système de traitement qu'il offre en service est conçu pour permettre des analyses de marché, pour communiquer des messages, pour dresser le profil de clients, etc.*")

[2232] B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, 70. Léonard and Mention point out that in such cases the controller's determination of means is only *indirect*: it is the processor who effectively determines the means of the processing, the controller only indirectly determines the means by choosing a particular processor. (T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 105.)

viewed primarily in this light. While certain language in Opinion 1/2010 can effectively be read as suggesting that the determination of (certain) means is optional in certain cases, earlier opinions (e.g., SWIFT, social networks) and other sections of Opinion 1/2010[2233] confirm that both a determination of both purposes and the means are (and remain) constitutive elements for control. Nevertheless, Van Eecke and Truyens rightfully draw attention to the inherent ambiguity of the approach developed by the Working Party, which will be elaborated further in the following section.

2.4 "MEANS"

1096. MEANS TO AN END – A controller must decide not only about the purposes of the processing of personal data, but must also decide about the means that shall be used to realise these purposes.

1097. "ESSENTIAL" VS. "NON-ESSENTIAL" MEANS – In Opinion 1/2010, the Article 29 Working Party introduced a distinction between "essential" and "non-essential" means.[2234] "Essential means", according to the Working Party, are those elements which are traditionally and inherently reserved to the determination of the controller, such as "*which data shall be processed*?", "*for how long shall they be processed*?", and "*who shall have access to them*?".[2235] "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software.[2236]

1098. RELEVANCE OF THE DISTINCTION – The Working Party attaches considerable weight to the distinction between essential and non-essential means. According to the Working Party, a determination of "means" only implies control when the determination concerns the essential elements of the means.[2237] Under this approach, the Working Party considers it possible that the technical and organisational means of the processing are determined exclusively by the data processor.[2238]

1099. MOTIVATION – The distinction between "essential" and "non-essential" means appears to have been motivated by practical considerations. In practice entities providing processing services often, at least to a certain extent, have a determinative influence over the means of the processing. As one scholar puts it, the determination of

---

[2233] See e.g. Opinion 1/2010, *l.c.*, 26.
[2234] See also *supra*; nrs. 93 et seq.
[2235] The Article 29 Working Party derived these criteria from the legislative development of the controller and processor concepts. As indicated earlier, previous iterations of the controller concept referred to four elements ("purpose and objective", "which personal data are to be processed", "which operations are to be performed upon them" and "which third parties are to have access to them"). According to the Working Party, the word "means" should be understood as comprising these elements. ("*[T]he final definition must rather be understood as being only a shortened version comprising nevertheless the sense of the older version.*") (*Ibid*, p. 14.)
[2236] *Id.*
[2237] *Id.*
[2238] *Id.*

the "means" of the processing *is* the service offered by a processor.[2239] One of the reasons why a controller may decide to enlist a processor is precisely because the controller lacks the technical expertise necessary to design and develop a processing system which is suited to his objectives.[2240] Absent any further threshold, *every* service provider offering standardised processing services which involve the processing of personal data might effectively be considered a controller.

1100. ISSUE – Although the Working Party has provided several examples to clarify the distinction between "essential" and "non-essential" means, the distinction can be difficult to apply in practice. After all, every choice of "means" serves to achieve a particular objective and may, depending on one's point of view, be considered "essential" in achieving that objective. This issue was implicitly acknowledged by the Working Party itself in Opinion 1/2010, in relation to the choice of security measures:

> "*In some legal systems decisions taken on security measures are particularly important, since security measures are explicitly considered as an essential characteristic to be defined by the controller. This raises the issue of which decisions on security may entail the qualification of controller for a company to which processing has been outsourced*."[2241]

Cloud computing services have put further pressure on the distinction between "essential" and "non-essential" means. Certain aspects of cloud computing services that are often determined by cloud providers (e.g., security measures, location of data, use of subcontractors, deletion processes, new service features, synchronisation services) may be considered as "essential" means.[2242] In this regard, the EDPS observed that

> "*More and more often, the determination of the essential elements of the means, which is a prerogative of the data controller, is not in the hands of the cloud client.*

[2239] T. Léonard, "'Data processor' and 'Data controller' - Are these concepts still adequate?", presentation held at the conference: "*Reinventing data protection*", Brussels, 12-13 October 2007, slide 9. See also T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 105 (« *Les moyens du traitement deviennent l'objet même du service fourni par les différents sous-traitants qui interviennent dans le processus de traitement. Ils sont déterminés par le seul sous-traitant comme élément essentiel de son service.* ») See also P. Van Eecke, M. Truyens et al. (eds.), "The future of online privacy and data protection", *l.c.*, 33.

[2240] See also A. Joint and E. Baker, "'Knowing the past to understand the present' - issues in the contracting for cloud based services", *Computer Law & Security Review* 2011, Vol. 24, Issue 4, 408.

[2241] Opinion 1/2010, *l.c.*, p. 15.

[2242] See also F. Gilbert, "Cloud service providers as joint-data controllers", *l.c.*, p. 9; W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 11. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", *l.c.*, p. 12 ("*...the complexity of the technical means used in the cloud environment has now reached such a stage that it is necessary to add that the cloud client/data controller may not be the only entity that can solely determine the "purposes and means" of the processing. More and more often, the determination of the essential elements of the means, which is a prerogative of the data controller, is not in the hands of the cloud client. In this respect, the cloud service provider typically designs, operates and maintains the cloud computing IT infrastructure*")

In this respect, the cloud service provider typically designs, operates and maintains the cloud computing IT infrastructure."[2243]

In its Opinion on cloud computing, however, the Article 29 Working Party did not, however, consider that the cloud provider's influence concerning essential elements of the processing automatically renders him controller. Rather, the Opinion indicated that as long as the cloud provider clearly outlines the essential elements of the processing in advance (and does not draw outside these lines without additional agreement from the customer), the provider may retain its status as processor.[2244] While the guidance of the Working Party is pragmatic, it also demonstrates that a number of grey areas remain, which may lead to divergent interpretations in practice.[2245]

2.4 "ALONE OR JOINTLY WITH OTHERS"

1101. TOGETHER OR ALONE – Article 2(d) of Directive 95/46 introduced a distinction between "joint" and "separate" control. Joint control exists where two or more actors share the same purposes and means of the processing in question. If the parties do not pursue the same purposes, or do not rely upon the same means for achieving their respective objectives, they are likely to be considered as "separate controllers" rather than "joint controllers".[2246]

1102. RELEVANCE OF THE DISTINCTION – The distinction between joint and separate control has significant practical importance with regard to liability exposure.[2247] In principle, collaborating separate controllers are only responsible for ensuring compliance of their own processing activities. A separate controller is generally not liable for acts or omissions committed by the other controller.[2248] In case of joint control, however, each controller is individually responsible for ensuring compliance of the processing as a whole. As a result, each joint controller can in principle be held liable for any damages resulting from non-compliance.[2249] The distinction between joint and

[2243] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", l.c., p. 12.
[2244] Cf. *supra*; nr. 962.
[2245] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 11.
[2246] Cf. *supra*; nr. 104. See also Opinion 1/2010, *l.c.*, 25.
[2247] In addition, article 24 of the draft GDPR requires that the respective responsibilities of joint controllers be determined by way of an arrangement between them (unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law).
[2248] T. Olsen and T. Mahler, "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *l.c.*, p. 41.
[2249] In Opinion 1/2010, the Article 29 Working Party considered that joint and several liability should only be imposed insofar as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances. (Opinion 1/2010, *l.c.*, p. 24.) As mentioned earlier, I do not believe the limitation provided by the Article 29 Working Party is entirely correct if one takes into account the general principles of European tort law (cf. *supra*; nr. 150). In any event, article 26(3) of the GDPR explicitly confirms that a data subject may exercise his or her rights under this Regulation in respect of and against each joint controllers irrespective of the terms of the arrangement between them.

separate control is also relevant in relation to basic controller obligations more generally, including the accommodation of data subject rights.

1103. ISSUE – The distinction between "joint" and "separate" control may be difficult to draw in practice. Joint and separate control reside at opposite ends of a continuum, with many possible variations between them. The notion of "partial joint control", as well as the recognition that joint control may be exercised "asymmetrically", at "different stages" and "to different degrees" clearly illustrate this point.[2250] Further confounding the analysis is the suggestion that control may be exercised only over certain *aspects* of the processing.[2251] While a granular application of the concept of "control" promotes flexibility, it also complicates matters. Establishing where the control of one party ends and another begins becomes increasingly difficult. Moreover, it increases the risk of confusion between two distinct issues: the legal status of an entity (as either controller or joint controller) and the legal implications associated with this status (i.e. the scope of its obligations).[2252]

2.5 "THE PROCESSING"

1104. OPERATION OR SET OF OPERATIONS – The decision-making power of a controller extends to the "processing" of personal data. The term "processing" is defined by article 2(b) as "any operation or set of operations" which is performed upon personal data. As result, the concept of a controller can be linked either to a single processing operation or to a set of operations.

1105. SUBJECT TO FRAMING – In situations where personal data is exchanged among multiple actors, the assessment of which actor (or actors) control(s) the processing hinges on the vantage point of the assessor. If "the processing" is considered from a very high level, i.e. as the entirety of operations that are needed to realize a particular service or output, one is likely to reach a different conclusion than if one were to "zoom in" on the individual processing operations which are performed to realize that service or output.[2253] As a result, practical difficulties might arise in determining whether a given

[2250] Cf. *supra*; nr. 103.
[2251] Cf. *supra*; nr. 772.
[2252] See also *infra*; nrs. 1132 et seq.
[2253] J. Alhadeff and B. Van Alsenoy, "Legal and Policy handbook for TAS^3 implementations", *Trusted Architecture for Securely Shared Services* (TAS^3), Deliverable 6.1-6.2, v1.0, 2012, p. 101. See also International Chamber of Commerce (ICC), ICC Task Force on Privacy and the Protection of Personal Data, "Summary of the Workshop on the Distinction between Data Controllers and Data Processors", Paris, Thursday, 25 October, 2007, p. 2 ("*Level of detail in analyzing the purposes and means of processing: Some participants indicated that decisions on the purposes and means of processing should be evaluated at each stage of the data processing chain, while others found that the overall picture of a data processing situation should be examined to determine whether a party was a data controller or a data processor.*")

series of operations should be considered as being part of the same "processing" or not.[2254]

1106. GUIDANCE - According to the Article 29 Working Party, the question of which entity is acting as a controller should be looked at "both in detail and in its entirety".[2255] Specifically:

> "*In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means.*"[2256]

The Working Party did not explicitly state when control should be assessed either at the level of a specific operation or set of operations. Its language suggests that the presence of a jointly defined purpose or use of jointly defined means should be determinative in deciding whether or not the processing should be assessed together or in isolation. An alternative approach would be to look at general perception. Given the central importance of the purpose specification principle to the regulatory scheme of EU data protection law, however, the delineation of "the processing" should be made in light of the purposes pursued.[2257] As Gutwirth argues:

> "*[T]he delineation and separation of purposes is decisive in the establishment of the number of processing operations. Finality is the key to pinpoint what the processing operation is. And since the whole protection system is engrafted onto the processing operation, it will succeed or fail based on the way in which processing is delineated. Personal data processing is each processing operation or series of operations with personal data which aims to realize one purpose, one finality.*"[2258]

1107. ASSESSMENT – The definition of processing as an operation or set of operations is beneficial. It promotes adaptability and allows a reasonable balance to be struck between two extremes: a separate controller for every processing operation and a single controller for all processing operations.[2259] Less straightforward, however, is the situation where personal data is not processed "as part of a chain", but rather as part of an integrated system (e.g., the IMI system).[2260] In such cases, control over "the

---

[2254] See also *supra*; nrs. 99 et seq. (noting that the delineation of "the processing" should in principle be made in light of the purposes pursued.)
[2255] Opinion 1/2010, *l.c.*, p. 3.
[2256] Opinion 1/2010, *l.c.*, p. 20.
[2257] Gutwirth, S., *Privacy and the information age*, *o.c.*, p. 97.
[2258] *Id.*
[2259] See also *supra*; nr. 466.
[2260] Cf. *supra*; nrs. 726 et seq.

processing" may be more difficult to determine, as different actors may control different *aspects* of the processing.[2261]

2.6 *"OF PERSONAL DATA"*

1108. OBJECT OF CONTROL – If an actor determines the purposes and means of the processing, but no personal data are involved, he or she will not be considered a controller. At least some of the data processed under the authority of a controller must relate to an identified or identifiable individual.

1109. KNOWLEDGE OR INTENT – The question may be asked whether it is necessary that the actor controlling the processing is *aware* of the fact that he or she is processing personal data. One could argue that in order to be considered a controller, the actor must exercise decision-making power towards the processing of data which it knows to be personal in nature.[2262] The Court of Justice implicitly rejected this argument, however, when interpreting the definition of "processing" in the context of *Google Spain*.[2263] As a result, an actor can be considered a "controller" even if he or she does not deliberately target personal data as such or is not a priori aware which data relate to identified or identifiable individual.[2264] This finding has implications not only for search engines, but also for other service providers such as online social networks and certain cloud providers.

1110. ISSUE – If an actor can be considered a controller without active knowledge of the personal data involved, the question arises as to how the absence of such knowledge may affect the scope of his obligations. At a practical level, the actor may not be able to comply with all controller obligations until he or she becomes (or is made) aware of the fact that personal data are involved. This issue was implicitly recognized in *Google Spain*, where the Court of Justice recognized that there may be practical limits to the ability of a search engine operator to meet all the obligations resulting from Directive 95/46.[2265]

[2261] Cf. *supra*; nrs. 771 et seq.

[2262] Google Spain SSRN paper, p. 16. See also Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraph 83.

[2263] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 28 (" … *regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.*").

[2264] In the same vein: P. De Hert and P. Papakonstantinou, "Comment – Google Spain -Addressing Critiques and Misunderstandings One Year Later", *Maastricht Journal of European and Comparative Law* 2015, Vol. 22, No. 4, p. 627 ("*'Knowledge' of the data controller or 'alteration' of the data, as Google contested, are not necessary conditions to this end.*").

[2265] In qualifying search engine providers as controller, the Court of Justice also immediately indicated that there may be limits to the obligations of search engines: "*[…] the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved*." (Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 38.)

2.7 "ON BEHALF OF"

1111. AGENCY – The definition of a processor states that a processor acts "on behalf of" a controller. The processor concept is frequently linked to the concepts of delegation and agency, understood as the process whereby one person (the principal) enlists another person (the "delegate" or "agent") to act on his behalf.[2266]

1112. CUMULATION POSSIBLE? – The criteria to determine whether an entity is acting as a controller or processor are not, by their nature, mutually exclusive. From a linguistic perspective, an actor can be involved in determining the purposes and means of the processing while at the same time acting "on behalf of" someone else. It is true that the legal definition of a processor implies that the processor is an entity separate from the controller, which would imply that the two roles cannot coincide (or at least not simultaneously). The linguistic criteria contained in the definitions of controller and processor, however, do not by themselves prevent cumulation.

1113. HYBRID ACTORS – Two of the use cases analysed in Part IV illustrate how certain actors combine the characteristics of both controllers and processors. In the e-Government setting, for example, the Pan-European Proxy Service could be viewed as either a controller or processor.[2267] Similar considerations apply in relation to certain cloud providers, who process personal data on behalf of their customers, while still exercising decision-making power regarding the purposes and/or means of the processing.[2268]

1114. SUBJECT TO FRAMING – In principle, once an actor is involved in determining the purposes and means of the processing, he or she must be deemed a (joint) controller - even if the processing itself is performed mainly to serve the interests of another party. In practice, however, regulators and scholars appear willing to accept that an entity may still be viewed as a "processor" even if it enjoys considerable latitude in deciding how the processing shall be organized.[2269] This has resulted in a situation where the assessment of the legal status of an entity may vary depending on which characteristics are perceived as dominant. If one emphasises the autonomy of the entity concerned (e.g., in designing and operating the service), or the limited choices available to end-users, one winds up concluding that the entity acts as a controller. Conversely, if one emphasizes the auxiliary nature of the service, designed to serve the interests of others, one winds up concluding that the entity should be deemed a processor. In other words: the final outcome of the analysis may be more a result of framing rather than the straight-forward application of established criteria.

[2266] Cf. *supra*; nr. 77 and nr. 437.
[2267] Cf. *supra*; nrs. 759 et seq.
[2268] Cf. *supra*; nrs. 918 et seq.
[2269] Cf. *supra*; nr. 962.

1115. ADDITIONAL CRITERIA – To help distinguish between controllers and processors, the Article 29 Working Party has developed a range of additional criteria. In Opinion 1/2010, for example, the Working Party mentions:

- level of prior instructions given (the greater the level of instruction, the more limited the margin of manoeuvre of the processor);
- monitoring of the execution of the service (a constant and careful supervision of compliance provides an indication of being in control of the processing operations);
- image given to the data subject; and
- expertise of the parties (if the expertise of the service provider plays a predominant role in the processing, it may entail its qualification as data controller).[2270]

1116. BALANCING TEST – None of the additional criteria developed by the Article 29 Working Party are by themselves determinative. Instead, the approach advanced by the Working Party seems to be more of a balancing test: the more elements there are pointing in favor of a particular qualification, the more likely it is that the "official" criteria (i.e., "purposes", "means", "on behalf") will be applied in a way that supports this qualification.

1117. CAVEATS – While the additional criteria provided by the Article 29 Working Party are helpful, a number of caveats can be made. First, not all of the additional criteria are anchored in the legal definitions of controller and processor. Second, the additional criteria can (also) be distributed among different actors. For example, even though the service provider might play a predominant role in the processing, the image given to the data subject might suggest another actor is in charge of the processing. Finally, the use of additional, non-determinative, criteria is likely to increase the role of framing.

1118. PRACTICAL IMPLICATIONS – The assessment of whether an entity is acting as a controller or processors requires careful appreciation of all the factual elements surrounding the processing. The criteria provided by the legal definitions of controller and processor may not always allow for a straight-forward determination. More often than not, the assessment will be driven by an overall assessment of the totality of circumstances, to determine the entity "should" be viewed as a controller or processor. The outcome of this assessment will inevitably be influenced by the teleological assumptions held by the adjudicator. This aspect will be developed further in the course of the following section.

[2270] Opinion 1/2010, *l.c.*, p. 28. See also *supra*; nr. 97.

3 TELEOLOGICAL

1119. PREFACE – The second category of issues arises from the teleological interpretation of the controller and processor concepts. The teleological method of interpretation involves interpreting a legal provision in light of the *original objectives* of the legislature (e.g., protecting certain interests, imposing a specific kind of behaviour).[2271] Applied to the controller-processor model, one can say that a teleological issue occurs when one or more of the objectives that underlie the controller and processor concepts are not fully realised in practice.

1120. METHODOLOGY – Part II of this thesis identified the various functions of the controller and processor concepts.[2272] It did not, however, elaborate *why* the EU legislature decide to introduce the distinction between controllers and processors in the first place. Therefore, this section must first clarify the policy objectives that underlie the distinction between controllers and processors. Relevant sources include the preparatory works of Directive 95/46, regulatory guidance issued by the Article 29 Working Party, the case law of the Court of Justice and doctrine. Once the underlying objectives have been identified, this section will assess to which extent these objective may not be fully realized in practice by drawing from the evaluation of use cases conducted in Part IV.

1121. OUTLINE – The preparatory works suggest that the primary aim of the differentiation between controllers and processors is to ensure a *continuous level of protection* in case of outsourcing. A secondary objective of the differentiation between controllers and processors is to provide *legal certainty* to the actors involved in the processing as regards the scope of their obligations. Finally, the case law of the Court of Justice indicates that the concept of a controller also seeks to ensure *effective and complete protection* of data subjects.

3.1 CONTINUOUS LEVEL OF PROTECTION

1122. COMMISSION PROPOSAL – While the initial Commission proposal for a Data Protection Directive did not contain a formal distinction between "controllers" and "processors", it did include a specific provision referring to persons or enterprises who process personal data "on behalf of" the controller. Article 22 of the Commission proposal provided that the controller may only outsource the processing of personal data to persons or enterprises which provide sufficient guarantees as regards the implementation of security measures.[2273] It also required the controller to conclude a

[2271] L. Kestemont, *Methods for traditional legal research*, *o.c.*, p. 12. See also and N. MacCormick, "Argumentation and Interpretation in Law", *l.c.*, p. 24-26.
[2272] Cf. *supra*; nrs. 188 et seq.
[2273] Article 22(1) of the Commission Proposal.

contract which specified the person or enterprise providing the processing service (as well as their employees) to confidentiality.[2274]

1123. EXPLANATORY MEMORANDUM – The Explanatory Memorandum accompanying the Commission proposal clarified the rationale behind article 22 as follows:

> "*The object of this article is to avoid a situation whereby processing by a third party on behalf of the controller of the file has the effect of reducing the level of protection enjoyed by the data subject. To that end, obligations are placed both on the controller of the file and on the third party carrying out the processing.*"[2275]

On the basis of this text, it seems reasonable to conclude that the primary rationale for introducing the distinction between controllers and processors was to ensure a continuous level of protection in case of outsourcing.[2276] While the initial Commission proposal foresaw imposing obligations directly upon processors, the final text of Directive 95/46 envisaged that continuous protection would be ensured by way of contractual safeguards, coupled with the liability of a controller for the actions of its processor.

1124. ACCOUNTABILITY TOWARDS DATA SUBJECTS – An important element of ensuring a continuous level of protection concerns the liability of controllers of controller for the actions of its processors. Even in case of outsourcing, the controller shall in principle remain accountable for any harm suffered as a result of unlawful processing. While the initial Commission proposal provided that the controller might be exempted from liability if he could demonstrate having taken appropriate measures (e.g., contractual binding, due diligence in choosing processors), the final text considerably narrowed the exemption (imposing strict liability).[2277] As a result, one could argue that an additional rationale underlying the distinction between controllers and processors was to reinforce the accountability of the controller of the processing towards data subjects, regardless of how the processing was organized. The imposition of liability upon the controller for the actions of its processor allows individuals to exercise their rights as data subjects with a single entity (the controller). By rendering a single actor responsible for ensuring compliance for the processing as a whole, the data subject is, at least in theory, spared the burden of determining the precise nature of the task allocation between the controller and processor. In case of harm, data subjects are

---

[2274] Article 22(3) of the Commission Proposal. Interestingly, article 22(2) provided that any person who collects or processes personal data on behalf of the controller must comply with the basic principles of data protection, suggesting that processors were equally responsible for compliance. Article 21, however, which concerned the issue of liability, only provided for liability of the controller.

[2275] Commission of the European Communities, "Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data", SYN 287, Explanatory Memorandum, p. 40.

[2276] See also Opinion 1/2010, *l.c.*, p. 25-26.

[2277] Cf. *supra*; nr. 126.

in theory also protected against the risk of being unable to determine whether the harm should be attributed to the controller or processor.[2278]

1125. STAYING IN CONTROL – Certain doctrinal accounts see an additional rationale behind the differentiation between controllers and processors, which is closely related to the desire to ensure a continuous level of protection. Specifically, it has been suggested the obligation of the processor to abide by the instructions of the controller is intended to ensure that the controller in fact remains "in control" of the processing.[2279]

1126. ISSUE – An implicit assumption of the controller-processor model of Directive 95/46 is that the controller is able to exercise control over the processing.[2280] The model assumes that whoever determines the "purposes and means" of the processing is effectively able to "take the lead" and ensure compliance with data protection requirements.[2281] After all, the idea of ensuring continuous protection by imposing strict liability upon controllers only makes sense if controllers can effectively adduce adequate safeguards.[2282] The processor, on the other hand, is implicitly viewed as being "non-autonomous", i.e. as merely executing instructions issued by a controller without substantially influencing the manner in which the processing shall be organized.[2283] In

---

[2278] In my opinion, this also explains why the Article 29 Working Party and national regulators consider "image given to data subjects" as a relevant factor in determining whether an entity should be considered as a controller or processor. Cf. *supra*; nr. 97.

[2279] See in particular T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 101-102 ("*La régime mise en place par la Loi à l'égard du sous-traitant vise à neutraliser les risques de l'intervention d'un tiers dans le traitement des données, et a perte potentielle de contrôle sur les données qui peut en résulter pour le responsable : le sous-traitant ne peut agir que sur instruction du responsable du traitement*") and P. Blume, "An alternative model for data protection law: changing the roles of controller and processor", *International Data Privacy Law* 2015, Vol. 5, No. 4, p. 294 ("*The well-known starting point is that the processor acts on behalf of the controller and that there must be a contract regulating the duties of the processor who furthermore has to be instructed by the controller. The processor has no independence and resembles an employee. This system is intended to ensure that the controller so to speak is in control and that there in principal is no difference between the use of internal and external helps.*")

[2280] See also P. Blume, "An alternative model for data protection law: changing the roles of controller and processor", *International Data Privacy Law* 2015, Vol. 5, No. 4, p. 292. ("*Data protection is founded on a fiction, at least to a large degree. The fiction is that the data controller is in control and is able to meet the obligations set out in the law. […] In order to believe in data protection law, it is necessary to believe that the controller is capable of performing the leading role in the play and act this role as it is written and thought.*")

[2281] M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *l.c.*, p. 26 ("*The notion of control […] does not belong to the granular reality of being in control but rather comes up as an expectation directed to whoever happens to "determine the purposes and means of the processing of personal data*"). One might also argue that definition of controller combines both factual ("is") and normative ("ought") components: the definition extends the object of the decision-making power to include elements over which the entity concerned should (normatively speaking) exercise decision-making power and take responsible decisions. Compare also *supra*; nr. 464 (discussing the CBPL proposal to extend the definition of controller under the Belgian data protection act, which was based on the consideration that certain aspects of the processing are important therefore the controller of the file "*should*" also have the power to decide about them).

[2282] P. Blume, "An alternative model for data protection law: changing the roles of controller and processor", *l.c.*, p. 292.

[2283] See also Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of

practice, however, the decision-making power of controllers is often constrained by the decisions made by processors, who autonomously design their services and offer them under standardised terms. The objective of ensuring continuous protection by way of contractual safeguards may therefore be undermined in practice in situations where controllers lack a sufficiently strong bargaining position or do not have the ability to choose from services which are compliant with EU data protection law. The cloud computing use case analysed in Part IV clearly supports this proposition.[2284]

3.2 LEGAL CERTAINTY

1127. CLARIFYING ROLES AND RESPONSIBILITIES – A second objective of the controller and processor concepts is to clarify the responsibilities of actors involved in the processing as regards the scope of their obligations.[2285] The concept of a processor, in particular, serves to identify the responsibilities of those processing personal data under the authority of the controller.[2286] This is closely related to the principle of legal certainty.[2287] By differentiating between controllers and processors, the EU legislature was able to delineate the (more limited) legal obligations incumbent upon those processing "on behalf of others". At the same time, it also allowed the legislature to clarify which measures controllers are expected to undertake when outsourcing data processing in order to ensure a continuous level of protection (i.e., due diligence, legal binding, oversight).[2288]

1128. ISSUE – The aspirations of legal certainty motivating the distinction between controllers and processors have not been realised in practice. The current uncertainty is

---

personal data", p. 2, available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf (last accessed 4 May 2016) ("*The definitions assume that a processor is an essentially passive entity, acting on behalf of a controller, with no independent influence over the way the processing takes place.*") and P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, p. 133-134 ("*[…] the Commission appears to uphold in its draft Regulation the aforementioned traditional personal data processing scheme, whereby roles are expected to be distinguishable and data processors are expected to be passive and of an executionary only function*").

[2284] See also P. Blume, "An alternative model for data protection law: changing the roles of controller and processor", *l.c.*, p. 294. See also See also Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", *l.c.*, p. 8 ("*The CSP may cease to be considered a processor, with all its consequences especially in terms of liability, in cases where the actions taken by the CSP exceeds by far the normal capacities of a data processor in viewed of its supposed absence of autonomy with respect to the instructions of the controller*".) Cf. *supra*; nrs. 941 et seq.

[2285] Opinion 1/2010, *l.c.*, p. 5.

[2286] Opinion 1/2010, *l.c.*, p. 5.

[2287] The principle of legal certainty is a general principle of EU law, which expresses the fundamental premise that those subject to the law must be able to ascertain what the law is so as to be able to plan their actions accordingly. (T. Tridimas, *The General Principles of EU Law*, 2nd edition, Oxford University Press, Oxford, 2006, p. 242 et seq.) See also J. Raitio, "The Expectation of Legal Certainty and Horizontal Effect of EU Law", in U. Bernitz, X. Groussot and F. Schulyok (eds.), *General Principles of EU Law and European Private Law*, Kluwer Law International, Croyden, p. 199-211.

[2288] Cf. *supra*; nrs. 82 et seq.

attributable in part to the nature of the existing concepts (cf. *supra*), but also - and perhaps to a larger extent - to the fact that the controller-processor model fits only a portion of the processing relationships that occur in practice.[2289] The controller processor-model only provides legal certainty in cases where the factual circumstances surrounding the processing can easily be mapped to the model and its implicit assumptions regarding autonomy and control. In other cases, the controller-processor model may actually create uncertainty, especially if the parties involved in the processing are unable to make an unambiguous determination regarding the legal status of each actor.[2290] Legal uncertainty increases, moreover, when the formal qualification established by parties involved in the processing does not withstand regulatory scrutiny and leads to requalification.[2291]

3.3 EFFECTIVE AND COMPLETE PROTECTION

1129. PRINCIPLE – The teleological method of interpretation has also been central to the reasoning of the Court of Justice in interpreting Directive 95/46.[2292] According to the Court of Justice, one of the objectives Directive 95/46 is to ensure the "effective and complete" protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.[2293] In *Google Spain*, the Court also explicitly referred to considerations of effectiveness in its interpretation of the controller concept:

> "*it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.*"[2294]

[2289] Several authors have argued that the controller-processor relationship reflects an outdated processing paradigm. Kuner, for example, has noted that the distinction between controllers and processors was far clearer the time the Directive was adopted. C. Kuner, *European Data Protection Law – Corporate Compliance and Regulation*, *o.c.*, p. 71-72. In the same vein, Moerel observes that *"At the time the first outsourcing transactions were concluded, it was indeed the controller who was in the driving seat as to imposing all terms relating to the outsourcing, including security requirements and whether data were transferred to non-EU countries or not. Today, with more commoditized outsourcing services [...] contractual terms on security and whether data transfers are taking place or not are (as much) dictated by the outsourcing supplier."* (L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 216)

[2290] See for example the discussion of the Pan-European E-Government service supra; nrs. 759 et seq.

[2291] See also L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 223.

[2292] See also D. Sancho-Villa, "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten", *l.c.*, p. 369.

[2293] Judgement in *Google Spain* C-131/12, EU:C:2014:317, paragraph 53. See also http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385

[2294] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 34. The principle of effectiveness, like the principle of legal certainty, is a general principle of EU law. The principle of effectiveness requires the effective protection of Community rights, including the effective enforcement of Community law in

1130. LIMITATIONS – The objective of ensuring "effective and complete" protection of individuals does not imply that each party involved in the processing of personal data must be subject to the same obligations. In *Google Spain*, for example, the Court of Justice also indicated that the burden incumbent upon search engines may be limited in light of their effective control capabilities:

> "*[…] the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.*" [2295]

1131. ISSUE – The approach of the Court of Justice in Google Spain has attracted considerable criticism. A first critique is that search engines are unable to comply with all of the obligations and restrictions that the Directive ordinarily imposes upon controllers.[2296] The second critique is that the approach of the Court of Justice may easily lead to inconsistent outcomes and therefore give rise to legal uncertainty.[2297] Strictly speaking, this critique does not concern the concepts of controller and processors themselves, but rather the implications associated with the concepts of controller and processor. This matter will be discussed further under the following section.

---

national courts. For a discussion see T. Tridimas, *The General Principles of EU Law*, *o.c.*, p. 418 et seq. See also N. Reich, "The Principle of Effectiveness and EU Private Law", in U. Bernitz, X. Groussot and F. Schulyok (eds.), *General Principles of EU Law and European Private Law*, Kluwer Law International, Croyden, p. 301-326.

[2295] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraphs 36-38. See also paragraph 34 ("*Furthermore, it would be contrary not only to the clear wording of that provision but also to its objective — which is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects — to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties.*").

[2296] While most of the provisions of Directive 95/46 allow for flexibility in their application, this is not always the case. See e.g. M. Peguera, "The Shaky Ground of the Right to Be Delisted", *l.c.*, p. 29 ("*Considering search engines as controllers is not without consequences, as they are unable to comply with most of the obligations the Directive imposes on data controllers.*"

[2297] *Id.*

4 SYSTEMIC

1132. PREFACE – The third category of issues arises from the systemic interpretation of the controller and processor concepts. According to the Court of Justice, provisions of Community law must be interpreted not only in light of its objectives, but also *in light of the "system" it establishes*.[2298] Where multiple interpretations are possible, practitioners must take into account the logic of the regulatory scheme established by the legislature.[2299] The systemic interpretation method involves taking into consideration the normative context in which a legal provision is placed and to derive logical consequences from other legal norms belonging to the same normative text.[2300] Systemic issues occur when the *functions* fulfilled by the controller and processor concepts give rise to unintended or undesirable consequences in practice, which in turn have an undue influence on the interpretation of the controller and processor concepts in specific instances ("strategic interpretations").

1133. OUTLINE – Part II of this thesis identified the various functions of the controller and processor concepts.[2301] As a matter of principle, each of the functions of the controller and processor concepts play a role in shaping their interpretation. Most relevant to the present analysis, however, is the function of these concepts in relation to (a) the transparency and data subject rights; (b) the scope of the obligations incumbent upon controllers; and (c) the degree of contractual flexibility in the relationship among actors involved in the processing of personal data.

4.1 TRANSPARENCY AND DATA SUBJECT RIGHTS

1134. THE DUTY TO INFORM – Every controller is in principle under an obligation to identify himself towards the data subject.[2302] One of the underlying objectives of this provision is to ensure that the data subject is aware of which entity is responsible for the processing, in order to allow him to exercise his rights as a data subject. In situations where a substantial number of (co-)controllers are involved, there is the risk that the data subject will not know to which entity to turn in order to exercise his rights, or from which entity he should seek redress in case of a privacy breach.

[2298] Judgement in *Satamedia*, Case C-73/07, EU:C:2008:266, paragraph 51.
[2299] See also G. Itzcovich, "The Interpretation of Community Law by the European Court of Justice", *German Law Journal* 2009, Vol. 10, No. 5, p. 549-557, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892093 (last accessed 22 February 2015) and N. MacCormick, "Argumentation and Interpretation in Law", *l.c.*, p. 22-23.
[2300] *Ibid*, p. 549.
[2301] Cf. *supra*; nrs. 188 et seq.
[2302] See articles 10-11 of Directive 95/46/EC (notice obligation).

1135. ILLUSTRATION – Cloud computing services can involve a large number of actors, whereby each actor is involved in the processing to varying degrees.[2303] If each of the actors involved in providing a cloud service were to be considered as a controller, it would substantially increase number of controllers involved in the processing. As a result, one might argue the risk would increase that the data subject will not know to which entity to turn in order to exercise his rights, or from which entity he should seek redress in case of a privacy breach.

1136. GUIDANCE – The fact that the multiplication of controllers may make it more difficult for data subjects to know who to turn to in order to exercise their rights, may unduly influence the interpretation of the controller concept. For example, in Opinion 1/2010, the Article 29 Working Party reasoned that :

> "*the assessment of joint control should take into account [...] that the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing.*" [2304]

1137. ISSUE – While the Working Party's statement appears to be consistent with the systemic method of interpretation, it also reveals a certain risk. The risk is that the concept of a controller is interpreted differently simply because of the increased number of actors involved in the processing. The legal status of an actor as controller or processor should in principle be determined in light of its actual role in the processing, not as a result of the number of actors involved in the processing. To hold otherwise risks undermining the "functional nature" of controller concept, which aims to allocate responsibility where factual influence is.[2305]

4.2 SCOPE OF OBLIGATIONS

1138. ALL OR NOTHING? – The obligations incumbent on a controller in principle befall the controller "as a complete set". A controller shall in principle be accountable for every aspect of the data processing: ranging from its obligation to ensure that the data quality principles are complied with, to the obligation to support the exercise of data subject rights, to notification obligations etc.[2306] In practice, the situation often occurs whereby certain obligations may more easily be fulfilled by entities other than the controller(s) himself (themselves). In Opinion 1/2010, the Working Party clearly emphasized that not being able to directly fulfil all the obligations of a controller does not excuse an entity

[2303] See also *supra*; nrs. 916 et seq.
[2304] Opinion 1/2010, *l.c.*, p. 24
[2305] Cf. *supra*; nr. 88.
[2306] Contra: Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 59-60.

from its obligations under data protection law.[2307] It may engage other actors to achieve compliance with its obligations, but this does not negate the fact that it is the controller that remains ultimately responsible for them.[2308] In other opinions, however, the Working Party has indicated that certain data controllers might be dispensed from complying with certain provisions in situations where these provisions are "not pertinent".[2309]

1139. ILLUSTRATION – Perhaps the best illustration is provided by the Opinion of the Article 29 Working Party on behavioural advertising.[2310] In this Opinion, the Article 29 Working Party considered the scope of the obligations incumbent upon website publishers in relation to the redirection of the browsers of internet users to the webpages (servers) of ad network providers. In this regard, the Working Party considered that:

> "*[...] publishers will have some responsibility as data controllers for these actions. This responsibility cannot, however, require compliance with the bulk of the obligations contained in the Directives. In this regard, it is necessary to interpret the legal framework in a flexible way by applying only those provisions that are pertinent. Publishers do not hold personal information; so obviously, it would not make sense to apply some of the obligations of the Directive such as the right of access. However, as further described below, the obligation to inform individuals of the data processing is fully applicable to publishers.*"[2311]

The guidance of the Working Party has far-reaching implications. It suggests that, in addition to the many different forms in which control might manifest itself (separate control, joint control, partial joint control), there might also be variation in terms of the scope of a controller's obligations. In other words, the Working Party's guidance could be read as suggesting that not every actor acting as a "controller" is necessarily bound to ensure compliance with all the obligations otherwise incumbent upon controllers.

1140. ISSUE – The aforementioned guidance of the Working Party further challenges the assumption that every controller must effectively be able to meet all of the obligations incumbent upon controllers.[2312] It also creates risk of undermining legal certainty.[2313] On the other hand, it seems that the number of situations in which it is

---

[2307] Opinion 1/2010, *l.c.*, p. 22.
[2308] *Id.* (stating "*It may be that in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller's behalf. However, a controller will remain in any case ultimately responsible for its obligations and liable for any breach to them.*").
[2309] Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", WP171, 22 June 2010, p. 11 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed 23 February 2016).
[2310] *Id.*
[2311] *Ibid*, p. 11-12 (emphases added).
[2312] Compare *supra*; nr. 1126.
[2313] Cf. *supra*, nr. 1127.

necessary to support greater flexibility in the application of controller obligations is increasing. In *Google Spain*, for example, the Court of Justice implicitly acknowledged that there may be practical limits to the ability of a search engine operator to meet all the obligations resulting from Directive 95/46.[2314]

4.3 LEGAL BINDING

1141. DIRECTIVE 95/46 – Article 17(3) of Directive 95/46 requires controllers to conclude a contract with their processors, which must specify that the processor is obliged (1) to follow the controller's instructions at all times and (2) to implement appropriate technical and organisational measures to ensure the security of processing. In contrast, Directive 95/46/EC does not contain any specific requirements aimed at regulating the relationship among controllers as such.[2315] The Article 29 Working Party has stated that controllers are free to determine how to best allocate responsibility amongst each other, "*as long as they ensure full compliance*".[2316] The result is that collaborating (co-)controllers are in principle free to assign responsibilities, whereas controller-processor relationships must be modelled according to a pre-defined format.

1142. NEGATIVE INCENTIVE – The regulatory scheme of Directive 95/46 incentivises service providers to structure their contractual relationships with customers as controller-processor relationships, because the status of processor entails fewer responsibilities and less liability exposure. In theory, following the controller-processor model also provides greater legal certainty for customers, who know exactly which contractual assurances must at a minimum be in place. The downside of this situation is that it may prevent actors involved in the processing from defining and allocating responsibilities in a way that more accurately reflects their respective effective control capabilities over (different aspects of) the processing. In other words, induces the creation of artificial contract clauses that exists primarily to sustain a legal fiction which does not necessarily correspond with reality.[2317]

1143. ONE SIZE FITS ALL? – The controller-processor model works well in situations where the relationship between the parties is consistent with the assumptions of autonomy and control that surround controller-processor relationship. The template is less useful, however, in cases where the relationship between actors is less "binary".[2318] In practice, only a portion of the processing relationships can easily be fitted into the controller-processor model. Relationships of joint control, separate control and partial

[2314] For a more narrow reading see M. Thompson, "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *l.c.*, p. 26.
[2315] One notable exception has resulted from the administrative practice surrounding international transfers. Cf. *supra*; footnote 189.
[2316] Opinion 1/2010, *l.c.*, 24.
[2317] A more favorable way to view such clauses is by qualifying them as "safeguards of the controller-processor relationship". Cf. *supra*; nr. 949.
[2318] See also *supra*; nr. 1128.

joint control are becoming increasingly common. The absence of similar recognition for contracts between joint controllers and collaborating single controllers may indirectly incentivize actors to model their contractual relationships according to the controller-processor template.

1144. IMPLICATIONS – The issue of contractual flexibility does not directly concern the concepts of controller and processor as such. Instead, it concerns the degree of prescription in regulating the relationship between controllers and processors. A possible remedy to the issue might consist of relaxing rigidity of controller processor template (e.g., by merely requiring controllers to "adduce adequate safeguards" when outsourcing personal data processing).[2319] Alternatively, or concomitantly, greater recognition could be given to other forms of collaboration (joint control, partial joint control) in order to signal that the controller-processor model is not the only way to structure the relationship between actors involved in the processing of personal data.

5 HISTORICAL

1145. PREFACE – The fourth and final category of issues arises from the historical method of interpretation of the controller concept. When applying the historical method, the interpreter tries to identify what the legislature wanted to regulate when using certain words and sentences, by *taking into account the historical elements that motivated the legislature's intervention*.[2320] Historical issues emerge when legal rules are applied to new actors or situations which were not envisaged by the legislature and which do not merit similar treatment.[2321]

1146. OUTLINE – Since the adoption of Directive 95/46, the processing capabilities of individuals have expanded considerably. Today, individuals enjoy processing capabilities which were initially the prerogative of large organisations, governments, and universities.[2322] This new reality has put considerable pressure on the framing of roles and responsibilities in Directive 95/46. Two issues in particular have come to the fore, namely:

(1) the rise of "amateur" data controllers, who process personal data relating to others outside a professional or organisational context ("democratisation of control"); and

[2319] Cf. *infra*; nrs. 1233 et seq.
[2320] W. Brugger, "Legal Interpretation, Schools of Jurisprudence, and Anthropology: Some Remarks from a German Point of View", *l.c.*, p. 397; L. Kestemont, *Methods for traditional legal research*, *o.c.*, p. 11.
[2321] For an example of an historical method of interpretation of the controller concept see Opinion of Advocate General Jääskinen in Google Spain, C-131/12, ECLI:EU:C:2013:424, paragraphs 77-81.
[2322] See e.g. J. Bing, "Data protection in a time of changes", *l.c.*, p. 247-248.

(2) the legal status of online service providers in relation to user-generated content.

5.1 THE DEMOCRATISATION OF "CONTROL"

1147. "PRIVACY 2.0" – The role of individuals has shifted. In less than 30 years, individuals have transcended their role as passive "data subjects" to become actively involved in the creation, distribution and consumption of personal data.[2323] Individuals share pictures, post videos and tweet reviews. Unless an exemption or derogation applies, individuals are – at least in theory – subject to data protection law. This hypothesis was confirmed early on by the *Lindqvist*[2324] ruling and more recently in *Ryneš*[2325]. Central to both cases was the question of whether the processing activities of an individual fell within the scope of article 3(2) of Directive 95/46, which exempts processing "*by a natural person in the course of a purely personal or household activity*".

1148. LINDQVIST – In *Lindqvist*, the Court of Justice put forth two criteria to determine whether the personal use exemption applies. In the first place the processing activity must be carried out "*in the course of private and family life*". Secondly, the exemption shall not apply where data are published on the internet and made accessible to an "*indefinite number of people*". The first component of the *Lindqvist* test is perhaps the most striking. Whereas article 3(2) of the Directive exempts data processing in the context of "*purely personal or household*" activities, the Court of Justice referred to activities carried out "*in the course of private or family life*". The latter wording is nowhere to be found in the text of Directive 95/46. The word choice instead seems to have been inspired by the language of article 7 of the EU Charter and/or article 8 of the European Convention of Human Rights.[2326] The allusion to this terminology appears to have been intentional. If so, it arguably has important ramifications for the scope of the personal use exemption. It has long been established that the protection of "private life" under article 8 ECHR is not restricted to that which has historically been dubbed "the private sphere". Rather, the European Court of Human Rights has repeatedly underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others.[2327] The second part of the *Lindqvist* test precludes its application in cases where data are made available to an "indefinite"

[2323] OECD, *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 2013, Paris, p. 32, available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last accessed 12 January 2015).

[2324] Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

[2325] Judgement in *František Ryneš*, C-212/13, EU:C:2014:2428.

[2326] Article 8(1) ECHR provides that "Everyone has the right to respect for his *private and family life*, his home and his correspondence". Article 7 of the EU Charter provides that "Everyone has the right to respect for his or her *private and family life*, home and communications."

[2327] See e.g. European Court of Human Rights, *P.G. and J.H. v. United Kingdom*, 25 September 2001, application no. 44787/98 at 56 and European Court of Human Rights, *Niemietz v. Germany*, 16 December 1992, application no. 13710/88, at 29.

number of people, yet does not specify a limit or threshold. The second part of the *Lindqvist* test is arguably most problematic.[2328] It implies, for example, that users of online social networks may be unable to invoke article 3(2) once the data in question passes a certain threshold of accessibility.[2329]

1149. RYNEŠ – The Court of Justice was called upon to interpret the scope of the personal use exemption for a second time in *Ryneš*, which concerned the use of video surveillance for home security purposes. [2330] The *Ryneš* Court held that continuous video surveillance of a public space cannot be regarded as a "purely personal or household" activity. According to the Court, the monitoring of a public space meant that the surveillance system was "*directed outwards from the private setting*" and therefore did not fall within the scope of article 3(2).[2331] In reaching its conclusion, the ECJ also took into account that (a) the objective of Directive 95/46 is to ensure a high level of protection[2332]; (b) any derogations and limitations must apply only in so far as is strictly

---

[2328] See also R. Wong and J. Savirimuthu, "All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet", *The John Marshall Journal of Information Technology and Privacy Law* 2008, Vol. 25, Issue 2. p. 246 ("*The ECJ's decision clarifies the extent to which individuals may be able to benefit from Article 3(2), when placing personal information on the Internet, however, it raises several questions. If it is accepted that limiting access of an individual's Web page to family members will be exempt from Article 3(2) DPD, such that the Data Protection Directive 95/46/EC does not apply, where does one draw the line for individuals whose web pages may extend beyond family members?*"); E. C. Harris, "Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have All the Answers", 22 *Am. U. Int'l L. Rev.* 2007, p. 787 and F.J. Garcia, "Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators", *Fordham Intell. Prop. Media & Ent. L.J.* 2005, Vol. 15, p. 1232 et seq.

[2329] Cf. *supra*; nr. 869 et seq. See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 103.

[2330] Judgement in *František Ryneš*, C‑212/13, EU:C:2014:2428. The facts in Ryneš were as follows: For a number of years, Mr. Ryneš had been plagued by attacks by unknown persons. The windows of the family home had been broken on several occasions. In order to protect his family and home, Mr. Ryneš decided to install a camera system. It consisted of one fixed camera which monitored the entrance to his home, as well as the public footpath and the entrance to the house opposite. Almost immediately, the camera system served its purpose. On the second night after its installation, one of the windows of Mr. Ryneš's home was broken by a shot from a catapult. The video recording made it possible to identify two suspects, which eventually led to criminal proceedings. When petitioned by one of suspects, the Czech Data Protection Authority (DPA) held that Mr. Ryneš's camera system violated the Czech data protection act. The main reasons were that (1) the camera system had captured, without consent of the individuals concerned, the images of people moving along the street or entering the house opposite; (2) Mr. Ryneš had failed to provide the individuals concerned any information regarding the processing of their personal data; and (3) Mr. Ryneš had failed to report the camera system to the DPA. Further legal proceedings ensued, resulting in a reference for a preliminary ruling to the ECJ. Could the processing carried out by Mr. Ryneš be classified as the processing of personal data "by a natural person in the course of a purely personal or household activity"?

[2331] Judgement in *František Ryneš*, C‑212/13, EU:C:2014:2428, paragraph 33. Specifically, the Court reasoned that "*To the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46.*" (*Id.*)

[2332] *Ibid*, at paragraph 27

necessary[2333]; and (c) the very wording of article 3(2) ("purely") also suggests it should be narrowly construed[2334].

1150. ISSUE – Data protection law has traditionally targeted governmental and commercial institutions as the main subjects of regulation.[2335] Although data protection law has evolved over time, it still reflects an organisational mindset.[2336] The highly technical manner in which many provisions have been drafted makes them a "poor fit" for regulating the activities of private individuals. The analysis of online social networks conducted in Part IV clearly illustrates this proposition.[2337]

5.2 CONTROL OVER USER-GENERATED CONTENT

1151. THE QUESTION OF "CONTROL" – Online platforms enable individuals to share information with essentially unlimited audiences. The role and responsibility of platform providers, such as online social networks or micro-blogging sites, has been a topic of much debate.[2338] A particular contentious matter is whether or not these providers should be considered as a "controllers" in relation to content shared spontaneously by their users. The analysis of online social networks in Part IV discussed the different ways in which this issue has been approached by scholars, courts and regulators.[2339]

1152. RELATIONSHIP DIRECTIVE 2000/31 – Closely related to the question of "control" is the issue of whether online platform providers can benefit from the liability exemptions contained in Directive 2000/31/EC. Sartor a.o. argue that online platform

---

[2333] *Ibid*, at paragraph 28-29.
[2334] *Ibid*, at paragraph 30.
[2335] J. Zittrain, *The Future of the Internet— And How to Stop It*, *o.c.*, p. 200. The reason is simple: computer usage started out as a prerogative of large companies, governments, and universities. See e.g. J. Bing, "Data protection in a time of changes", *l.c.*, p. 247-248. For discussion of the availability and main forms of usage of computer systems in the 1970's see Commission des Communautés Européens, "Systèmes à grande puissance de traitement automatique de l'information. Besoins et applications dans la Communauté européenne et au Royaume-Uni vers les années soixante-dix", *Études*, Série Industrie, n° 6, 1971, p. 39-57. See also V. Mayer-Schönberger, "Generational Development of Data Protection in Europe", *l.c.*, p. 223 and C. Reed, "The Law of Unintended Consequences - Embedded Business Models in IT Regulation", *Journal of Information Law and Technology* 2007, vol. 2, paragraph 33, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/reed/reed.pdf (last accessed 17 January 2014).)
[2336] See also M. Birnhack, "Reverse Engineering Information Privacy Law", *l.c.*, p. 64 et seq. and C. Reed, "The Law of Unintended Consequences - Embedded Business Models in IT Regulation", *l.c.*, in particular paragraphs 26 through 39.
[2337] Cf. *supra*; nr. 871.
[2338] See e.g. D. Keller, "Intermediary Liability and User Content under Europe's New Data Protection Law", *Center for Internet and Society (CIS) Blog*, Stanford Law School, 8 October 2015, available at http://cyberlaw.stanford.edu/blog/2015/10/intermediary-liability-and-user-content-under-europe%E2%80%99s-new-data-protection-law (last accessed 29 February 2016).
[2339] Cf. *supra*; nrs. 874 et seq. The *Google Spain* ruling offers further support for proposition that certain OSN providers should be considered as "controllers" in relation to user-generated content, as they are actively involved in determining visibility of content (e.g. through so-called "timelines" or "newsfeeds" and by offering search functionalities).

providers should in principle be able to avail themselves of these provisions, including in situations where the dispute concerns the unlawful processing of personal data.[2340] Others have argued that article 1(5)b of Directive 2000/31/EC precludes the application of the liability exemptions in matters governed by Directive 95/46/EC.[2341]

1153. RELEVANCE – From the perspective of a data subject seeking to obtain removal of online content, it matters little whether the takedown is performed pursuant to Directive 95/46 or Directive 2000/31. Insofar as the unlawful dissemination of personal data is considered as "illegal content or activity" within the meaning of article 12 of Directive 2000/31/EC, the data subject should be able to request removal under both instruments. From the perspective of the provider, however, the applicability of the liability exemptions contained in the E-Commerce Directive may be considered as beneficial. Keller, for example, argues that the standard of care incumbent upon "controllers" is more onerous (and therefore more likely to give rise to liability) than the standard of care incumbent upon internet intermediaries.[2342]

[2340] See e.g. G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *l.c.*, p. 5 et seq.; G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 573 et seq. M. V. de Azevedo Cunha, L. Marin and G. Sartor, " Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2012, Vol. 2, No. 2, p. 57-58.

[2341] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 60-61.

[2342] See D. Keller, "Intermediary Liability and User Content under Europe's New Data Protection Law", *l.c.*, FAQ 2 ("*[…] parts of the GDPR seemingly create liability for intermediaries even when they are unaware that they are processing content unlawfully. Such a departure from the eCommerce Directive's knowledge standard would be a sea change for intermediary liability, and make the operation of open platforms for users to receive and impart information a much riskier business.*") Keller also points out that the size of possible penalties under the GDPR may provide an added incentive for intermediaries to "overcomply" with removal requests.

Chapter 3 TYPOLOGY OF SOLUTIONS

1 INTRODUCTION

1154. PREFACE – Over the past decade, a number of solutions have been put forward to remedy the issues that surround the application of the controller-processor model. The aim of this Chapter is to introduce and discuss the proposed solutions in light of the issues identified in the previous chapter. Where appropriate, additional solutions, not previously put forward, will be discussed as well.

1155. CATEGORISATION – In order to facilitate the comparison of possible solutions in relation to the issues identified in Chapter 2, the solutions will be categorized in the same manner as the typology issues presented in the previous chapter:

(1) *Grammatical solutions*: proposals that involve changing the words chosen to define the concepts of controller and processor;

(2) *Teleological solutions*: proposals that present alternative ways in which the policy objectives underlying the controller and processor concepts might be realized;

(3) *Systemic solutions*: proposals that involve modifying the implications associated with the concepts of controller and processor;

(4) *Historical solutions*: proposals that seek to confine the scope of application of the controller and processor concepts to actors and situations envisaged by the legislature.

1156. INTERDEPENDENCIES – While maintaining the categorisation above promotes consistency in presentation, it is obvious that a proposed solution might seek to address multiple issues. It is equally possible that a solution seeking to address one issue may indirectly ameliorate or exacerbate other issues, without deliberately seeking to do so. With this in mind, the potential solutions will be categorized according to the type of issue that is the *focal point* of the proposed solution. Where interdependencies exist, the discussion of each solution will involve an assessment of whether the solution is likely to improve or aggravate other issues.

1157. METHODOLOGY – The solutions analysed in this Chapter have been sourced from literature concerning the application controller and processor concepts, as well as from the stakeholder responses and legislative proposals put forward in the context of the review of Directive 95/46. Not every issue identified in Chapter 2, however, has been explicitly addressed by scholars or stakeholders. Where no remedy has been put forward, possible solutions will be developed in light of the lessons learned from

historical-comparative analysis and by drawing inspirations from approaches adopted by other national and international privacy frameworks.[2343]

1158. POSITIVE ASSESSMENT FRAMEWORK – The typology of issues set forth in Chapter 2 shall serve as the *positive assessment framework* to evaluate the proposed solutions.[2344] Each proposal will be evaluated in light of issue it seeks to remedy, simply by asking the following questions: how likely is the proposed solution to solve the identified issue? What are the advantages and disadvantages of this approach? In principle, no additional assessment criteria will be used to evaluate the proposed solutions. Only in the context of the internal comparison between different possible solutions, shall insights from the field of law and economics be applied in order to enhance the evaluation process.

1159. LIMITATIONS – The choice has been made to limit the evaluation of possible solutions to solutions proposed in the context of the review of Directive 95/46 and by academic literature. Only in cases where no proposal has been put forward to identify a particular issue shall additional solutions be developed and evaluated. As result, there can be no pretence at exhaustivity. Moreover, the proposed solutions discussed here have each been put forward in relation specific issues that arise under the current framework. As such, the proposals focus primarily on remedying identified problems and not on preserving or enhancing the beneficial properties of the current framework. Nevertheless, by analysing each of the proposals put forth during the review of Directive 95/46, it is possible to provide greater insight into the policy choices made by the European legislature. Moreover, by contrasting the proposals with the typology of issues, it will be possible to perform an informed evaluation of those choices and to develop recommendations for areas in which further improvement is still possible.

[2343] For reasons of accessibility, analysis has been limited to privacy frameworks available in English. In the end, the German *Bundesdatenschutzgesetz* of 1977 and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) of 2000 acted as additional sources of inspiration, as they contain interesting alternative approaches to the identification of responsible actors and regulation of outsourcing arrangements.

[2344] According to Kestemont, a "positive assessment framework" can be described as "*a set of criteria that are being formulated in a 'positive way'. This implies that the outcome of the evaluation will be positive or favourable when the legal phenomenon meets (nearly) all criteria.*" (L. Kestemont, *Methods for traditional legal research*, *o.c.*, p. 31.)

2 GRAMMATICAL

1160. OUTLINE – Grammatical solutions consist of modifying or clarifying the words that have been used to define the concepts of controller or processor. The point of departure is that if the current wording gives rise to difficulties of interpretation, the remedy is to modify this wording. Proposed solutions include (a) removing words from the definition of controller; (b) adding words to the definition of controller; and (c) substantively modifying the definition of controller.

2.1 DELETION OF "MEANS"

1161. PROPOSALS – Prior to the First Reading of the General Data Protection Regulation, several Parliamentary Committees proposed to remove the word "means" from the definition of a controller.[2345] The IMCO Committee explained the proposal as follows:

> *"With new technologies and services available such as cloud computing traditional division of entities involved in the processing of personal data may prove difficult, with the processor having in such cases significant influence over the way in which data are being processed. For this reason it seems reasonable to determine the controller as the entity, which decides over the purpose of processing personal data as determination of finality is the most important decision with the other factors serving as means to achieve it."*[2346]

The deletion of "means" was also supported by the authors of an External Report commissioned by the Parliament, who argued that abandoning the "means" criterion would be advisable because*:*

- *"there are substantial doubts as how to understand the term "means";*
- *greater importance is already assigned to the factor of "determining the purposes" rather than "determining the means" of processing;*

[2345] See European Parliament, Opinion of the Committee on Industry, Research and Energy (ITRE), 26 February 2013, Amendment 80; Opinion of the Committee on Internal Market and Consumer Affairs (IMCO), 28 January 2013, Amendment 62; Opinion of the Committee on Legal Affairs (JURI), 25 March 2013, Amendment 38 and European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendments 746-48 .

[2346] European Parliament, Opinion of the Committee on Internal Market and Consumer Affairs (IMCO), 28 January 2013, amendment 62. In the same vein, MEP Adina-Ioana Vălean, Jens Rohde argued that "*The definition of controller should be based on the decision of the purposes for which personal data are processed rather than the conditions or means by which this is achieved. The control over the purpose for processing is the logical basis for allocating different responsibilities between controllers who are responsible for what and why data is processed and processing parties who deal with how data is processed.*" (European Parliament, LIBE Committee, "Amendments 602-885", 4 March 2013, PE506.145v01-00, amendments 746). Other MEP's supported the change for a different reason, namely to clarify that only the controller and not the processor is responsible for compliance (See MEP amendments 748, with justification that: "*The aim of the change is not to lower the level of protection for the individual but to clarify that only the controller and not the processor is responsible. See related Amendments to articles 22, 24, 26 and 77.*")

- *Article 29 Working Party even permits the possibility of "delegation" of the competence to determine the means to the processor (at least as defined by the narrow meaning of that term);*
- *moreover, the general importance of "purposes" of processing is much higher in the personal data protection regulation because – as the legal literature reasonably notes – "the finality pursued by (a set of) processing operations fulfils a fundamental role in determining the scope of the controller's obligations, as well as when assessing the overall legitimacy and/or proportionality of the processing*".[2347]

1162. RATIONALE – The reasoning of the IMCO Committee reveals a dual motivation behind the proposal to delete the word "means" from the definition. The first motivation is that it would clarify that the determination of "purpose" is what really matters (primacy of purpose).[2348] The second motivation stems from the finding that providers of processing services often exercise significant influence over the way in which data are being processed. Removal of the word "means" would signal a desire to exclude such service providers from the scope of the controller concept. In other words, it would imply that service providers who effectively determine the "means" of the processing (but have limited interest in the purposes pursued by their clients) should no longer be qualified as (co-)controllers.[2349]

1163. COUNTERARGUMENTS – Despite its many supporters, the proposal to delete the word "means" was received negatively by the European Data Protection Supervisor (EDPS). In particular, the EDPS considered that the word "means" should not be deleted as it "*effectively contributes to the understanding and delineation of the roles of controller and processor*". [2350] A second counterargument may be derived from the guidance of the Article 29 Working Party, which emphasizes the *functional nature* of the controller concept. According to the Working Party, the aim of the controller is to allocate responsibility upon those actors who exercise factual influence over the processing. Retaining the word "means" would make it easier to keep actors who exercise significant influence over the way in which data are being processed within the scope of the controller concept.[2351] The need to hold service providers accountable for aspects of the

---

[2347] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31, with reference to B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *l.c.*, p. 31, footnote 55.
[2348] See also *supra*; nrs. 92 et seq.
[2349] See also MEP amendment 748, which justified the deletion of means as follows: "*The aim of the change is not to lower the level of protection for the individual but to clarify that only the controller and not the processor is responsible. See related Amendments to articles 22, 24, 26 and 77*."
[2350] European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", 15 March 2013, p. 6 (at paragraph 24), accessible at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf (last accessed 20 October 2015).
[2351] See also *supra*; nr. 633.

processing which are effectively under their control was also highlighted by report of the CEPS Digital Forum on the data protection reform.[2352]

2.2 *ADDING "CONDITIONS"*

1164. PROPOSAL – In its draft proposal of the GDPR, the European Commission extended the definition of controller to include a reference to "conditions". The controller would be the entity who not only determines the "purposes and means" of the processing, but also the "conditions" of the processing. Neither the Commission Communication nor the Explanatory Memorandum offer any further clarification regarding the underlying rationale for this proposal.

1165. COUNTERARGUMENTS – The authors of the External Report commissioned by the Parliament put forward a number of arguments against the Commission Proposal. First, it is unclear how the term "conditions" should be understood, if it were expected to have a different meaning or connotation what is already covered by the word "means".[2353] Second, the use of the conjunction "and" would imply a requirement of cumulative satisfaction. This might actually trigger greater difficulties and uncertainties of interpretation, rather than eliminate them.[2354]

2.3 *"BENEFIT-BASED" APPROACH*

1166. PROPOSAL – A third proposal consists of substantively modifying the definition of the controller concept. In 2008, authors Léonard and Mention proposed to define the controller as the entity that *benefits from the use of data*, rather than as the entity who "determines purposes and means" of the processing.[2355] The proposal is closely tied to the observation that the constitutive element of the processor concept is that this entity processes personal data *on behalf of* the controller:

> "*If the processor only processes data on behalf of the controller, it may be appropriate to focus the distinguishing criterion for the controller the identification of he who benefits from the use of data and in this sense really decides about the purposes of their use. The processor certainly profits and benefits from the treatment that is the very purpose of his service, but he does not draw as such profit from the use itself of data for the information they contain.*"[2356]

[2352] K. Irion and G. Luchetta, "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), *l.c.*, p. 47-48.
[2353] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 30.
[2354] *Id.*
[2355] T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 109.
[2356] *Id.* (original emphasis)

1167. RATIONALE – Léonard and Mention depart from the observation that the existing criteria no longer work in practice. The "means" criterion is deemed inadequate, because in practice almost every processor exercises a determinative influence over the manner in which the processing is organised.[2357] The "purpose" criterion is likewise deemed inadequate, because in practice every processor designs and offers his services with a particular finality in mind (and in that sense can always be seen as determining the "purpose" of the processing).[2358] By differentiating on the basis of "who receives the benefit from the use of the data", it is argued, it is possible to operate a much neater distinction between controllers and processors.

1168. COUNTERARGUMENTS – While the proposal of Léonard and Mention was not formally discussed in the context of the GDPR negotiations, its rationale and intended effect are similar to the proposal to delete the "means" criterion.[2359] As a result, similar countervailing arguments can be made. If adopted as such, the proposal would entail that the providers of processing services would effectively be excluded from the concept of a controller, even if they exercise a determinative influence over the manner in which the processing is organised (including the "essential elements" of the processing). Absent additional measures, there is a risk that the providers of processing services may lack appropriate incentives to organise their services in a manner which sufficiently takes into account the interests of data subjects.[2360]

2.4 ASSESSMENT

1169. INTERNAL COMPARISON – Of the three proposals presented discussed above, the "benefit-based" approach seems most apt to introduce greater clarity in the distinction between controllers and processors. It is indeed difficult to imagine how the proposal to add "conditions" would assist in disambiguating the controller concept.[2361] Merely deleting the "means" criterion would likewise be too subtle a change, especially in light of the fact that scholars continue to associate multiple meanings to the "purpose" criterion.[2362] The "benefit-based" approach would support a relatively clear distinction between actors who provide processing services ("processors") on behalf of others and

[2357] *Ibid*, p. 105
[2358] *Ibid*, p. 107.
[2359] The main difference is that the proposal of Léonard and Mention would further substitute the "purpose" criterion with a reference to "who benefits from the use of the data". However, the rationale offered by proponents of the proposal to delete the "means" criterion implicitly suggests these proponents also understand the "purpose" criterion as referring to "interest in" or "benefit from" the processing. For a more detailed discussion of the interpretation of purpose as "interest" vs. "finality" see *supra*; nrs. 959 et seq.
[2360] See also K. Irion and G. Luchetta, "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), *l.c.*, p. 47-48.
[2361] First, as indicated earlier, it is unclear how the word "conditions" would add meaning beyond what is already included by the word "means". In addition, the more cumulative criteria are enumerated in a single definition, the more likely one is to find that they are not united in a single entity (compare also *supra*; nr. 464)
[2362] Cf. *supra*; nrs. 959 et seq.

actors who consume them in the pursuit of their own organisational objectives ("controllers"). An additional advantage of the benefit-based approach is that it would introduce a mutually exclusive criterion in the definitions of controller and processor.[2363]

1170. INTERDEPENDENCIES – Adoption of the "benefit-based approach" would affect the teleological issues identified in Chapter 2. On the one hand, by offering a clearer basis for differentiation between controllers and processors, the benefit-based approach would arguably improve legal certainty. On the other hand, the benefit-based approach could adversely affect the objective of the EU legislature to ensure a continous level of protection by responsibilizing actors who exercise a determinative influence over the manner in which the processing is organized. By excluding the providers of processing services from the scope of the controller concept, such service providers may not be sufficiently accountable for their decisions regarding how the processing should be organized. Additional measures may therefore be necessary to address this issue. Finally, it is worth noting that the benefit-based approach would leave unaffected the systemic and historical issues identified in Chapter 2.

1171. ACCOUNTABILITY GAP – A benefit-based approach would only be acceptable if additional measures are put in place to ensure the providers of processing services are accountable for the manner in which they decide to organise their processing services. As noted by the Report of the CEPS Digital Forum on the data protection reform:

> "*[T]he means of data processing carries a stand-alone risk for the protection of personal data; important procedural aspects and decisions are deployed, such as algorithms. Regulation should therefore not be blind to the means even if this aspect of data processing is no longer under the exclusive control of the controller. Here, parallel to reducing the level of responsibility on the part of the controller, accountability on the part of the processor would need to be stepped up.*"[2364]

In other words, it would be necessary for the EU legislature to impose additional obligations directly upon the providers of processing services to ensure accountability in relation to those aspects of the processing which are effectively under their control. Failure to do so would make it increasingly difficult for regulators to exert influence over essential elements of the processing which can otherwise create stand-alone data protection risks. Relevant obligations (which might be imposed directly upon processors) include: the obligation to implement appropriate security measures, the obligation to implement data protection by design and by default, the duty to respect

[2363] As indicated earlier, the current criteria to distinguish between controller and processors are not mutually exclusive. Cf. *supra*; nr. 1112.

[2364] K. Irion and G. Luchetta, "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), l.c., p. 47-48. While these observations were made in relation to the proposal to remove the word "means" from the definition of controller, similar considerations also apply in relation to the interest-based approach. Compare also *supra*; nr. 424.

international transfer restrictions, and the obligation to co-operate with supervisory authorities.[2365]

1172. REMAINING ISSUES – While the "benefit-based" approach makes it easier to differentiate between controllers and processors in most cases, its application may not always be equally straight-forward. Considering the fact pattern in *Google Spain*, for example, it could be argued that the provider of a search engine service is not the ultimate "beneficiary" of the service he provides. As a result, it might be argued that the provider of a search engine service should no longer be considered as a "controller". Such an outcome would stand in stark contrast with the reasoning of the Court of Justice, who considered it necessary to qualify search engines as controllers in order to ensure "effective and complete" protection of data subjects.[2366] Similar objections might also be made in relation to data brokers, whose data processing activities have the potential to significantly affect the privacy interests of data subjects, but are the ultimate "beneficiaries" of the data services they offer to their customers.[2367]

1173. FINAL TEXT GDPR – The final text of the GDPR left the controller and processor concepts "as is". Given the extremely broad scope ratione materiae of the Directive, a certain amount of legal uncertainty appears inevitable.[2368] Even if the criteria set forth by article 2(d) were to be rephrased, the need for continuous adaptability would most likely lead to wording which still leaves room for legal uncertainty in some cases. Practitioners may therefore simply have to accept a certain amount of ambiguity in the criteria set forth by the regulatory framework, and plan accordingly.[2369] Chapter 4 will nevertheless present a proposal for possible revisions to the controller and processor concepts, based on the solution proposed by Léonard and Mention.

[2365] It is worth noting that each of the obligations mentioned here were included in the list of obligations which would be imposed upon processors under the First Reading of the European Parliament. Under the General Approach of the Council, however, the number of obligations directly incumbent upon processors was substantially reduced (e.g., data protection by design and by default).

[2366] Cf. *supra*; nr. 1053.

[2367] A possible remedy might be to specify that, in order to be considered a processor, the party must process the data "exclusively on the instructions of" or "exclusively at the request of" another party (in addition to processing the data exclusively on his behalf). Cf. *infra*; nr. 1260.

[2368] See also Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paragraph 86: "*As regards Directive 95/46 itself, its provisions are necessarily relatively general since it has to be applied to a large number of very different situations.*"

[2369] See also C. Kuner, *European data protection law: corporate compliance and regulation*, *o.c.*, p. 72.

3 TELEOLOGICAL

1174. OUTLINE – Teleological solutions are solutions which propose alternative ways in which policy objectives underlying the controller and processor concepts might be realized. The point of departure is that if the current approach fails to achieve important policy objectives, it is necessary to consider alternative approaches to realise those objectives. Proposed solutions include (a) abolishing the distinction between controllers and processors or (b) increasing the number of obligations directly incumbent upon processors.

3.1 ABOLITION OF THE DISTINCTION

1175. PROPOSAL – Proposals to abolish the distinction between controllers and processors can be traced back as early as 2007, to a workshop organized by the ICC Task Force on Privacy and the Protection of Personal Data.[2370] The summary report of the workshop notes that:

> "*Abolition of the distinction between controller and processor: Some participants stated that the distinction between data controller and data processor is artificial, and it would be preferable to have a single category of party processing personal data whose rights and obligations are determined under the facts in each case and in accordance with general legal principles; other participants disagreed with this proposal.*"[2371]

While not all the workshop participants shared the view that the distinction between controllers and processors should be abolished, the proposal was further developed by the ICC itself in its response to the European Commission consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data:

> "*The distinction between "data controller" and "data processor" should be abolished, and each party that processes personal data should be responsible and liable based on its own role in the data processing. […] Existing concepts of agency law and tort law already provide a sufficient legal framework for assessing the responsibility of parties involved in data processing, without forcing them into a limited set of categories that does not fit reality.*" [2372]

[2370] International Chamber of Commerce (ICC), ICC Task Force on Privacy and the Protection of Personal Data, "Summary of the Workshop on the Distinction between Data Controllers and Data Processors", Paris, Thursday, 25 October, 2007, 6 p.

[2371] *Ibid*, p. 2.

[2372] International Chamber of Commerce (ICC), ICC Commission on E-business, IT and Telecoms, "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", December 2009, p. 4, available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/international_chamber_of_commerce_icc_en.pdf.

1176. VARIATIONS – Proposals to abolish the distinction between controllers and processors were also made by other respondents to the aforementioned EC consultation, as well as by academics.[2373] There are, however, notable variations among the proponents of this approach, not least as regards the question of how responsibility and risk should be allocated under the revised model. The ICC, for example, advocated that each party involved in the processing of personal data should only be responsible and liable "*based on its own role*" in the processing. The law firm of Bird & Bird argued that the liability exposure of organisation involved in the processing of personal data should be limited "*to the extent of its legal right to control the data and to the extent necessary to secure the fundamental rights of the individual*".[2374] De Hert and Papakonstantinou, on the other hand, implied that each entity involved in the processing might be held equally accountable:

> "*perhaps the preferable way forward would be for the Commission to boldly abolish the notion of "data processors" from its Regulation altogether, and vest the data controller title, rights and obligations upon anyone processing personal information, regardless of its means, conditions or purposes.*"[2375]

The International Pharmaceutical Privacy Consortium considered that parties involved in the processing of personal data should be free to *designate* which party will be legally accountable, as long as the designated party has a European presence or has appointed a European representative."[2376] Finally the UK Information Commissioner's Office suggested that general liability might be assigned to the organisation(s) that *initiate* the processing, whereas anyone *subsequently involved* in the processing of personal data at a later stage would only be liable "*for their own aspect*" of the processing.[2377]

[2373] See Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, at paragraph 19; European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 5 and P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.* p. 134.

[2374] Specifically, Bird & Bird advocated "*to replace the distinction of controllers and processors with a principle that any organisation processing personal data should be liable to comply with the data protection principles but only to the extent of its legal right to control the data and to the extent necessary to secure the fundamental rights of the individual*." (Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, at paragraph 22. The European Privacy Officers Forum similarly reasoned that "*[p]robably the only practical approach is to make any party processing personal data liable for compliance with the rules, but only to the extent necessary to safeguard personal information in respect to a particular processing operation, and to the extent of that person's legal right to control the data.*" (European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 9.

[2375] P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, 133-134.

[2376] International Pharmaceutical Privacy Consortium, "Comments in Response to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, p. 7.

[2377] Specifically, the ICO reasoned that "*Rather than trying to keep rigid definitions, better data protection is achieved by making sure that any new legal framework clearly identifies the persons responsible for the various aspects of the processing of the data, and that the responsibility remains in place throughout the information life cycle. Liability could be assigned to the organisation, or organisations, that initiate the processing, whereas anyone processing personal data at any stage of the information life cycle should be*

1177. RATIONALE – One of the objectives underlying the controller-processor distinction was to clarify the obligations of each actor involved in the processing of personal data.[2378] Each of the proponents cited above elaborated at length as to why they believe this objective is no longer realised in practice. In general, most proponents argued that the distinction reflects an outdated paradigm, which is overly simplistic and has become increasingly difficult to apply in practice.[2379] Some even suggested that, because of its decreased relevance and applicability, the distinction actually *creates* confusion and imposes excessive interpretation costs.[2380] Abolishing the controller-processor distinction mainly seeks to remedy this situation. In addition, it could also provide greater flexibility to the parties involved in the processing of personal data to determine how to mutually allocate responsibilities.

1178. COUNTERARGUMENTS – The proposal to abolish the distinction between controllers and processors was met with caution. For example, the External Report commissioned by the European Parliament stated that:

> *"Such solutions, however, also entail certain far-reaching consequences in the form of, for example, making the positions of all entities involved in data processing equal and distributing all the obligations evenly, without taking into account their individual position, the scope of their tasks, or the expectations of data subjects. Therefore, the possible adoption of such solutions requires far-reaching prudence."*[2381]

---

responsible for dealing with it properly and securely, and be accountable for their own aspect of the processing. This could mean being accountable to whoever initiated the processing; to individuals; to regulators; or all three." (Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data", 2009, p. 2-3, accessible at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf (last accessed 9 March 2016).

[2378] Cf. *supra*; nrs. 1127 et seq.

[2379] See e.g. Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data", *l.c.*, p. 2-3; P. De Hert and V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *l.c.*, 133-134 and European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 5.

[2380] European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 5; Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, at paragraph 19 ("*The SWIFT case also demonstrates the amount of time and effort that is required to determine who is a controller and who is a processor (with organisations potentially having different roles depending on each individual act of processing). This diverts resources away from more substantive compliance requirements"*). See also International Pharmaceutical Privacy Consortium, "Comments in Response to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", l.c., p. 7 ("*A great deal of time and effort is spent trying to determine the appropriate categorization of the parties involved in a data processing activity, and it is reasonable to question whether this time might be better spent actually ensuring that appropriate data privacy and security safeguards are in place."*)

[2381] X. Konarski, D. Karwala, H. Schulte-Nölke and C. Charlton, "Reforming the Data Protection Package", *l.c.*, p. 31.

The authors of the External Report did not explore the possibility of combining the abolition of the controller-processor concepts with alternative criteria for allocating responsibility and risk. It was implied, however, that it may be possible to achieve similar outcomes, provided the current framework is interpreted properly:

> "*[I]t seems that, on the basis of the dichotomy adopted in EU law, one can – with proper interpretation – achieve results similar to those found in regulations [which do not make a distinction between controllers and processors].*"[2382]

3.2 OBLIGATIONS FOR PROCESSORS

1179. PROPOSAL – Under Directive 95/46, processors are in principle only indirectly accountable for compliance.[2383] The Directive itself specifies only one obligation directly towards the processor, namely in article 16. Article 16 provides that the processor may only process personal data pursuant to the instructions of the controller.[2384] In its draft proposal for the GDPR, the Commission significantly expanded the number of obligations incumbent upon processors. Specifically, the Commission envisaged that the following provisions would also be directly applicable to processors: (a) the obligation to maintain documentation; (b) the duty of co-operation with supervisory authorities; (c) the obligation to maintain an appropriate level of data security; (d) data protection impact assessments; (e) prior authorization; data protection officers; (f) codes of conduct; certification; and (g) international transfers. [2385]

1180. RATIONALE – The Commission's proposal was grounded in the view that, despite the increased complexity of the environment in which controllers and processors operate, the concepts themselves remain valid.[2386] Rather than abolish the distinction, the Commission would "clarify and detail" the responsibilities and liability of both controllers and processors.[2387] While the Commission's stated intent was to enhance legal certainty, it would appear that the approach proposed by the Commission was motivated by other factors as well. In its detailed analysis of impacts accompanying the proposal, the Commission reasoned that

---

[2382] *Id.* One of the regulations referred to by the authors is the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), according to which responsible organisations must take all reasonable steps to protect personal information under their control, regardless of where it is processed. For a discussion see also B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *l.c.*, p. 41-42 and J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 55-56.

[2383] Cf. *supra*; nrs. 117 et seq.

[2384] In addition, the processor shall in principle be obligated to observe all relevant aspects of data protection law by virtue of the contract which must be concluded among controllers and processors (article 17(3)).See also Opinion 1/2010, l.c., 26 and T. Olsen and T. Mahler, "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' - Part II", *l.c.,* p. 418.

[2385] Cf. *supra*; nr. 533.

[2386] European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2, *l.c.*, p. 10.

[2387] *Id.*

> "*New and harmonised provisions which clarify the legal obligations for the processor, irrespective of the obligations laid down in the contract or the legal act with the controller, as well as the application of the "data protection by design" principle, the need for data protection impact assessments in some cases, and an obligation to cooperate with supervisory authorities will bring about benefits for the individual, as this will ensure that outsourcing and delegation by controllers to processors do not result in lowering the standard of data protection.*"[2388]

As noted by the EDPS, imposing obligations directly upon processors more accurately reflects the "*growing role of processors in determining certain essential conditions of the processing*".[2389] In addition, doubts have been expressed whether the "contractual approach" of Directive 95/46 (whereby processors are obligated to observe relevant aspects of data protection law by virtue of their contract with the controller) actually creates the best incentives for compliance.[2390] The finding that certain organisations who are traditionally viewed as controllers (e.g., the customers of cloud services), often have a weak bargaining position in practice, undoubtedly provided additional motivation for the decision to increase the number of obligations directly incumbent upon processors.[2391] Finally, as indicated earlier, it has been argued that the choice of "means" of the processing creates a stand-alone risk for data protection for which processors should also be accountable.[2392]

1181. COUNTERARGUMENTS – The approach put forward by the European Commission was not entirely well received. Certain commentators felt that by imposing obligations directly on processors, there may be a risk of confusion as to who is ultimately responsible for ensuring compliance.[2393] For example, in relation to the data security obligation (article 30), the EDPS noted that:

[2388] European Commission, "Detailed analysis of impacts", Annex 5, *l.c.*, p. 91.

[2389] European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", *l.c.*, at paragraph 25.

[2390] L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 216-218 ("*Thought should be given to the question whether the present set-up of the Directive where the controller is the sole bearer for all data protection obligations is indeed the best incentive to achieve compliance in case of complex data processing operations. In light of the diminishing contracting power of multi-nationals vis-à-vis their multinational outsourcing suppliers, an obligation on all parties involved in the data processing (whether controller or data processor) to achieve accountability as to the end result, may ultimately prove the better stick. This may work as an incentive for all parties to come to a proper allocation of obligations in relation to the network. By separating the contractual form from the liability regime, it is left to the parties to allocate responsibilities where they are best placed.*" (original emphasis) Moerel goes on to advocate in favor of allocating responsibility *at the source of the risk*, rather than through a chain of contracts along the supply chain. The obligation to ensure data security should in particular be imposed directly upon processors (in addition to data controllers (*Ibid*, p. 222).

[2391] *Ibid*, p. 216. Blume even goes so far as to suggest that, in light of the increased dominance and effective control capabilities of processors, it should be considered whether the current roles of controllers of processors might be reversed. See P. Blume, "An alternative model for data protection law: changing the roles of controller and processor", *l.c.*, p. 295-297.

[2392] K. Irion and G. Luchetta, "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), *l.c.*, p. 47-48. Cf. *supra*; nr. 1171.

[2393] See in particular P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 143-144 and B. Treacy, "Challenging times ahead for data processors", *l.c.*, p. 5-6.

> "*In Article 30 on security of processing, reference is made to the controller and the processor. The EDPS welcomes that both actors are mentioned, but recommends the legislator to clarify the provision in such a way that there is no doubt about the overall responsibility of the controller. From the text as it currently stands, both the processor and the controller seem to be equally responsible. This is not in line with the preceding provisions, in particular Articles 22 and 26 of the proposed Regulation.*"[2394]

In the same vein, the ICO noted in relation to article 26 (processor) that

> "*[…] we need to be clear about who is responsible for what where a number of organisations are each involved in the processing of personal data, and, as drafted, this Article will not help us here.*"[2395]

While supporting the idea of directly imposing the obligations upon processors, Moerel has argued that the approach of the European Commission failed to provide adequate flexibility as far as the mutual allocation of responsibility and risk is concerned.[2396]

3.3 ASSESSMENT

A. Abolition of the distinction

1182. ADVANTAGES – The proposal to abolish the distinction between controllers and processors has considerable appeal. It would eliminate from the legal framework an artificial construct which has given rise to considerable difficulties of interpretation. From a purely practical perspective, the need to appropriately divide responsibilities exists regardless of whether the relationship between the actors involved is a relationship between controller and processor, separate controllers or (partial) joint

---

[2394] European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", *l.c.*, p. 31 (at paragraph 192). See also P. Blume, "Controller and processor: is there a risk of confusion?", *l.c.*, p. 144.

[2395] Information Commissioner's Office (ICO), "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper", *l.c.*, p. 34. At the same time, the ICO also reiterated its earlier complaint regarding its difficulties to distinguish between controllers and processors in practice ("*It is fair to say that the ICO can find it difficult to determine which organisations are data controllers and which are processors. The problem arises because, given the collaborative nature of modern business, it is rare for a one organisation (the processor) to only act on instructions from another (the controller). There tends to be a considerable degree of freedom, skill, judgment and the like in terms of the way the first organisation provides services to the second, all against the backdrop of complex collaborative arrangements involving numerous organisations.*") (*Id.*)

[2396] L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 218 ("*I agree that the imposing of direct obligations on processors is a good way to ensure that processors in complex processing operations do not "hide" behind their processorship in order to avoid liability. However, if the Proposed Regulation allows joint controllers to divide responsibilities between them, I do not see why this possibility would not be extended to a division of responsibilities between joint processors (or between main and sub-processors) ad further between (joint) controllers and such (joint or sub-) processors. If individuals keep their rights against any of them, there seems little to be said against such possibility to divide responsibilities.*")

controllers. By abolishing these distinctions, parties can focus immediately on how to best allocate responsibilities.

1183. DISADVANTAGES – There are, however, a number of disadvantages to this approach. First, while parties no longer need to invest time and energy debating their formal legal status, there is still a need to allocate responsibilities. Removing the distinction between controllers and processors would remove an important "guidepost" as to what an appropriate allocation of responsibilities might look like.[2397] Moreover, one should not lose sight of the fact that the controller-processor relationship is in fact a *normative* construct: by regulating the relationship between controllers and processors, the EU legislature has not merely indicated what the contractual relationship might look like, it is also an indication of what the relationship *should* look like.[2398] Finally, allocating responsibility and risk may prove more difficult in practice. As indicated earlier, there are different opinions as regards the question of how responsibility and risk should be allocated in absence of the controller-processor model. Some appear to favour an equal distribution among those involved in the processing, others argue that responsibility and risk should be allocated in function of the specific "role" assumed by the actor in question. The benefits and drawbacks specific to each approach will be analysed over the following paragraphs.

i. Equal distribution (joint and several liability)

1184. BASIC PRINCIPLE – Equal distribution of responsibility and risk would imply that each party involved in the processing is subject to liability exposure for the whole of the processing, regardless of its specific function. It closely resembles a "strict" liability regime, whereby mere "involvement" in an unlawful processing activity may be sufficient to trigger liability exposure towards data subjects. While the party who is thus held liable may be able to take recourse against another party pursuant to the their internal distribution of risks, any party who is thus held liable is obliged to indemnify the data subject and might potentially be subject to administrative penalties.[2399]

[2397] Of course, data protection authorities could still provide similar guideposts when interpreting other provisions which contain open-ended obligations (e.g. the duty to take "all appropriate measures" to ensure confidentiality and security of processing). Such guidance, however, would not enjoy the same legal weight as a statutory provision.

[2398] Under the controller-processor model, service providers who act as processors are contractually bound to limit the further use of data to purposes specified by the customer. Controllers, on the other hand, are in principle free to reuse data for their own purposes provided those purposes are compatible or they have consent. In other words, the controller-processor model may help to slow down function creep.

[2399] In principle, the liability exposure of each party under the equal distribution model may be either proportional (each party's liability exposure is limited to their proportional share in causing the damages or in light of the severity of their faults) or joint and several (each party's liability exposure towards the data subject is for the whole amount of the damages, regardless of the nature of fault or contribution). For purposes of conceptual clarity, the proportional liability model shall be discussed separately. Cf. *infra*; nrs. 1187 et seq.

1185. ADVANTAGES – From the perspective of the data subject, equal distribution of responsibility and risk offers a number of benefits. First, it provides data subjects with maximum protection against insolvency of any of the parties involved in the processing. Second, it completely removes the burden from data subjects to ascertain who is "ultimately" responsible for the damage. In situations where there is no clear indication of which party should be accountable to data subjects, this is a significant advantage. Third, imposing risk upon any actor involved in the processing could also provide data subjects with considerable economies of scale. For example, if a data subject would be able to exercise the right to object with the major providers of processing services (who offer their processing services to a large number of customers), the data subject would be relieved from the burden of contacting customers of the processing service individually.

1186. DISADVANTAGES – For all its advantages, equal distribution also displays considerable disadvantages. First, imposing the same obligations and liability exposure upon every actor "involved" in the processing, no matter how remotely, is likely to be excessive in many cases.[2400] Second, the transaction cost for the providers of processing services would increase exponentially, given their increased liability exposure. The probability of litigation, with the attendant negative publicity, is likely to induce certain service providers to become highly selective with their clientele.[2401] Third, an equal imposition of responsibility and risk would effectively force providers of processing services to become more involved in the processing they would otherwise be.[2402] Service providers might even be called upon to interfere in the internal relationship between their customers and the data subjects involved, a relationship which is essentially foreign to them.[2403] Moreover, there is the risk that the parties hold different views as to how compliance should be achieved, or as to how a data subject request should be resolved. Such differences in opinion between the parties involved in the processing may put a considerable strain on their commercial relationship. While the authority to make decisions on data subject requests may be allocated internally between the

[2400] For example, a telecom provider is strictly speaking also "involved" in the processing conducted using a cloud service, but the provider may not have actual or constructive knowledge of the processing of personal data taking place, nor have any relationship with the data subjects concerned. In the same vein, a PaaS cloud provider may strictly speaking also be "involved" in the processing undertaken by third-party application providers, but may have no knowledge or relationship with the data subjects concerned. See also W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 18 et seq.

[2401] This may make it more difficult for smaller and less-established companies to find processing partners.

[2402] For example, the staff of a cloud provider might de facto be required, in the context of an exercise of data subject rights, to access and scrutinize information they otherwise would not seek access to.

[2403] See also T. Léonard and A. Mention, "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", *l.c.*, p. 108. Not being a direct party to the commercial, legal or other relationship between the customer and the data subject, he providers of processing service may be ill-placed to judge the propriety of the processing or determine whether or not to accommodate a particular request made by a data subject,

parties, the risk of liability exposure may render certain providers uncomfortable with leaving such decisions in the hands of their customers.[2404]

ii. Role-based accountability (proportional liability)

1187. BASIC PRINCIPLE – An alternative to the equal distribution model is the model of "role-based accountability". Instead of imposing equal responsibility and risk upon each of the actors involved in the processing, proponents of this approach advocate allocating responsibility and risk in function of the "role" of each party involved in the processing.[2405] Under this model, liability can be either strict or negligence-based, but it is any event "proportional" rather than joint and several or vicarious.[2406]

1188. ADVANTAGES – A major benefit of the role-based model is that every party involved in the processing shall only be accountable in light of its *actual* role in the processing. The scope of a party's responsibilities can be determined completely in light of the degree of control each party exercises in practice. In theory, it is also possible to differentiate according to different aspects of the processing: one party might, for example, be functionally responsible for security, while another might be responsible for ensuring data accuracy. From a fairness perspective, this is a significant improvement over the equal distribution model, as in principle each party shall only be exposed to liability in light of its effective control capabilities.

1189. DISADVANTAGES – While the role-based model provides advantages over the equal distribution model, it also displays a number of flaws. As a preliminary matter, however, it is worth observing that each of the proposals mentioned above fails to offer a clear alternative standard for allocating responsibility. It is simply envisaged that the scope of a party's responsibility should be determined in light of its "role" or "control". The role-based model therefore does not solve the difficulties regarding the concept of "control", it simply moves the question to a later stage in the analysis.[2407] *Chassé par la porte, il revient par la fénêtre*. One could even argue that the role based-model is not actually a solution, but simply a restatement of the policy objectives underlying the

---

[2404] There is also the question of how meaningful transparency can be ensured in a model where every actor involved in the processing would in principle be obliged to disclose its identity and purposes pursued when processing the data. In principle, the parties involved could designate a party among themselves, as suggested by the International Pharmaceutical Privacy Consortium (cf. *supra*; nr. 1176). However, granting parties the same flexibility as regards liability exposure and the duty to accommodate data subject rights is less straightforward. If the parties are given complete freedom to designate who shall be responsible, the stronger party will almost inevitably seek to transfer responsibility to the weaker party, which may not appropriately reflect their respective control capabilities.

[2405] Cf. *supra*; nr. 1176.

[2406] Under proportional liability, each party's liability exposure is limited to their proportional share in causing the damages. If one party proves insolvent, the loss shall in principle be borne by the data subject. By contrast, in case of joint and several liability, each party can be held liable by data subjects for the full amount. See also J. Boyd and D.E. Ingberman, "The 'Polluter pays principle'": Should Liability be Extended When the Polluter Cannot Pay?", *The Geneva Papers on Risk and Insurance* 1996, Vol. 21, No. 79, p. 184

[2407] In other words: while the concept of "control" is no longer applied as a factor to determine the formal status of an actor, it remains equally relevant to establishing the scope of each party's obligations.

controller-processor model (i.e., to allocate responsibility with those entities that exercise factual influence over the processing). The role-based model also raises questions as regards incentives: if the scope of a party's obligations are determined purely in light of its actual role, there is a risk that parties will "do less" to ensure compliance with data protection responsibilities.[2408] Last but not least, the role-based model is unlikely to provide effective remedy for data subjects. On the contrary, data subjects may experience greater difficulties in obtaining redress, as they risk carrying the burden of demonstrating that a party should have done more in light of its "role" or "degree of control" (which may be more onerous than demonstrating the exercise of a determinative influence over the purpose and means" of the processing).

iii. Combined approach (general and proportional liability)

1190. BASIC PRINCIPLE – The "combined approach" consists of assigning general liability to one party (for the processing as a whole), whereas anyone involved in the processing of personal data at a later stage is accountable for their own aspect of the processing.[2409] The party that is assigned general liability might, for example, be the party that "*initiates*" the processing[2410] or, alternatively, the party who has the "*primary relationship*" with the data subject[2411]. The party who is assigned general liability is liable for any processing activities undertaken on its behalf, whereas the other parties shall only be proportionally liable in light of their role. Liability in principle is not joint and several, except possibly in cases of jointly committed faults or where different faults contribute to the same damage.[2412]

1191. ADVANTAGES – The combined approach displays a number of advantages over the previous two models. It incorporates, for the most part, the benefits of the role-based approach (proportional liability), but also ensures the data subject is in a position

---

[2408] After all, the more they do, the more likely they are in considered to be in control of those aspects of the processing.

[2409] See e.g. W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 24-25 ("*we advocate a more flexible approach, which may impose primary liability on one party, but assign different degrees of responsibility and liability to other actors in proportion to the individual parts they each play in the processing chain*")

[2410] The ICO proposed assigning liability "to the organisation, or organisations, that initiate the processing, whereas anyone processing personal data at any stage of the information life cycle should be responsible for dealing with it properly and securely, and be accountable for their own aspect of the processing. This could mean being accountable to whoever initiated the processing; to individuals; to regulators; or all three." (Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data", *l.c.*, p. 2-3.

[2411] Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, at paragraph 20 (the authors themselves immediately dismissed the proposal as it inapplicable in contexts such as law enforcement) (*Ibid*, at paragraph 21).

[2412] As we will be discussed later, the combined approach closely resembles the approach ultimately taken by the EU legislature under the GDPR. The main difference is that the GDPR retained both the concepts of controller and processor, which enables it to differentiate among the obligations incumbent upon each party involved in the processing. Cf. *infra*; 1215.

to seek remedy from a single actor in relation to every aspect of the processing. The combined approach also has the advantage that it is consistent with the general principles of tort law.[2413] Finally, the combined approach represents only a minor change in relation to the controller-processor model of Directive 95/46. The data subject enjoys the same recourse capabilities vis-à-vis the party who is assigned general liability as it would against controllers and joint controllers. In addition, there is an explicit recognition that the data subject may also hold other parties accountable for those aspects of the processing for which they are responsible. This is an improvement over the current model, as it removes the possibility for service providers to "hide" behind their processor status when confronted with a liability claim (which under Directive 95/46 is a possibility in jurisdictions where processor liability is not recognised).

1192. DISADVANTAGES – The limitations of the combined approach are similar to those of the role-based model. First, proponents of the combined approach fail to provide a clear alternative standard that could realistically replace the current criteria for control. While the concept of "initiation" has a strong appeal (reference to initiation has also been made in the interpretation of the controller concept[2414]), it may not scale well in the case of multiple collaborating controllers, whereby one controller independently decides to re-use data for a separate purpose.[2415] Imposing general liability upon the party who has the "primary relationship" with the data subject works relatively well in the business-to-consumer (B2C) context, but presents difficulties in situations where the party behind the processing does not have a direct relationship with the data subject (e.g., law enforcement agencies, data brokers, search engines).[2416] Second, the combined approach does not specify how the obligations of other parties involved in the processing of personal data shall be determined. It is simply envisaged that each party shall be accountable in relation to its "own aspect" of the processing, without specifying which data protection obligations may be viewed as relevant in relation to a particular aspect of the processing.

iv. Interdependencies

1193. GRAMMATICAL ISSUES – Abolishing the distinction between controllers and processors would theoretically solve the grammatical issues associated with the concepts of controller and processor. As indicated earlier, however, it would create a need for alternative criteria - and hence vocabulary - to determine which obligations

[2413] Cf. *supra*; nrs. 132 et seq.
[2414] Cf. *supra*; nr. 70.
[2415] If it is argued that such re-purposes is tantamount to "initiating" a new form of processing, it is clear that the "initiation" approach is in fact equivalent to the current approach (which hinges on the decision to process personal data for a particular purpose).
[2416] See also Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", *l.c.*, at paragraph 22 ("*It would also be unlikely to translate easily outside the consumer arena because if, for example, data are processed by law enforcement agencies without the individual's knowledge, then talk of a 'primary relationship' would seem strained*").

apply to which party. Alternatively, the same vocabulary and criteria might be implemented in a later stage of the analysis (e.g., by using the criterion of "control" when assessing the scope of liability of a party involved in the processing as opposed determining whether the party falls within the remit of the controller concept).

1194. SYSTEMIC ISSUES – Abolishing the distinction between controllers and processors would have implications for provisions which hinge (or have hinged) upon the distinction between controllers and processors, namely (a) applicable law; (b) scope of obligations; (c) transparency; (d) data subject rights; (e) interest balancing and (f) legal binding. For purposes of conceptual clarity, the relationship with systemic issues will discussed in the next section (cf. *infra*).

1195. HISTORICAL ISSUES – Abolishing the distinction between controllers and processors could potentially aggravate certain historical issues. Absent additional measures, it would increase the likelihood of directly imposing the full panoply of controller obligations upon actors who fulfil an intermediary role or otherwise facilitate the dissemination of content shared by their customers.

B. Obligations for processors

1196. ADVANTAGES – The benefits of imposing additional obligations on processors are essentially three-fold. First, in comparison with the proposal to abolish the distinction between controllers, this approach represents a much less radical departure from the current framework. Existing case law and regulatory guidance concerning the controller and processor concepts remain relevant. Second, imposing additional obligations directly upon processors renders the obligation to comply with (certain) data protection requirements independent of the prior conclusion of a contract between controllers and processors. As indicated earlier, this is especially relevant in situations where controllers are in a relatively weak bargaining position. Third, this approach partially reduces the practical importance of the distinction between controllers and processors. As a result, establishing whether a party to the processing is acting as a controller or processor becomes less of an "all or nothing" exercise. Regardless of legal status, certain basic obligations are directly applicable to both controllers and processors.

1197. LIMITATIONS – Two of the three advantages outlined in the previous paragraph only apply insofar as obligations are in fact imposed directly upon processors. If an obligation is not imposed upon processors (e.g., data protection by design and by default), there shall be limited or no possibility of holding processors accountable for those aspects of the processing (unless the obligations are imposed by way of contract). Any discrepancies may still influence the interpretation of the controller and processor concepts. A second limitation (or benefit, depending on one's perspective) is that the

approach does not completely remove the need to further specify distribution of tasks. For example, if both controllers and processors are subject to obligation to ensure security, in practice there is still a need for further task distribution as to which party will take care of which security requirements (e.g., enforcing access control privileges vs. assigning access control privileges).[2417] Finally, it is worth noting that it might not always be appropriate to impose the same obligations on all providers of processing services.[2418]

1198. INTERDEPENDENCIES – Imposing obligations directly upon processors reduces certain systemic issues, as the applicability of certain obligations is no longer contingent upon legal status. Absent further measures, however, other systemic issues remain unaffected. Grammatical issues regarding the distinction between controllers and processors remain the same, as do the historical issues that arise when applying the controller and processor concept to contexts not anticipated by the EU legislature.

C. Internal comparison

1199. PROBLEM STATEMENT – Each of the proposals presented above has its merits and limitations. Abolishing the distinction between controllers and processors would theoretically decrease the associated interpretation costs, but requires an alternative mechanism to allocate responsibility and risk. The question of which approach is best suited for purposes of data protection law is (at least in part) a question as to the *optimal degree of differentiation and specificity* of data protection law. To develop this point further, it is necessary to first clarify the distinction between two types of legal pronouncements, namely "standards" and "rules".[2419]

i. Standards vs. rules

1200. BASIC PROPERTIES – A *rule* is a legal pronouncement which states a determinate legal result that follows from one or more well-specified triggering facts.[2420] A *standard*, in contrast, puts forward a legal or social criterion that legal decision-makers ("adjudicators") use in order to judge actions under particular circumstances.[2421]

[2417] One could argue that this limitation also exists under Directive 95/46 and therefore does not constitute a disadvantage compared to the current state of affairs.

[2418] Cf. *infra*; nr. 1208.

[2419] See also B. Coene, *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, Proefschrift aangeboden tot het behalen van de titel van Doctor in de Rechten aan de KU Leuven en de UGent, Academiejaar 2015-2016, p. 221-249 and p. 347-362.

[2420] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *Oregon Law Review* 2000, Vol. 79, No. 1, p. 23.

[2421] V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", Law and Economics Working Paper Series 04-32, George Mason University School of Law, 2007, p. 4, available at http://www.law.gmu.edu/assets/files/publications/working_papers/04-32.pdf (last accessed 14 March 2016). See also R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p.

Standards indicate the types of circumstances that are relevant to a decision on legality, but remain relatively open-ended.[2422] Rules, on the other hand, withdraw from the consideration of the decision-maker one or more circumstances that would be relevant to decision-making according to a standard.[2423] An example may serve to better illustrate the distinction between standards and rules. The legal pronouncement that "*in case of outsourcing, every controller must bind its processors by way of a contract or legal act specifying at a minimum [xyz]*" is essentially a rule. It clearly specifies the situation in which the rule is to take effect and enumerates its consequences. On the other hand, the legal pronouncement that "*every actor involved in the processing of personal data shall take every reasonable measure to ensure adequate protection of personal data, including in case of outsourcing*" is a standard rather than a rule.

1201. A FALSE DICHOTOMY – Rules and standards reside at opposite ends of a continuum.[2424] In practice, the difference between rules and standards is a question of degree rather than a binary distinction.[2425] The greater its specificity, the more a legal pronouncement approximates a rule. The more it allows for flexibility in its application (e.g., through qualifications, exceptions, or criteria), the more a legal pronouncement resembles standard.[2426] A multi-factor balancing test can display both rule- and standard-like properties. Depending on the degree of specificity with which the facts relevant to the legal determination are specified in advance, it shall resemble a rule to a greater or lesser extent.[2427]

1202. BENEFITS AND COSTS – Rules and standards each have associated benefits and costs.[2428] Generally speaking, detailed rules are often considered inflexible, unable to cope with change, and quickly outdated.[2429] Broad standards, on the other hand, support flexibility and adaptability, but can result in uncertainty, inconsistent application and

---

23. ("*Standards [...] require legal decision makers to apply a background principle or set of principles to a particularized set of facts in order to reach a legal conclusion*").

[2422] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *The Journal of Legal Studies* 1974, Vol. 3, No. 1, p. 258.

[2423] *Ibid*, p. 258. See also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 4. Another way to distinguish rules from standards is by looking at the extent to which "*efforts to give content to the law are undertaken before or after individuals act*". See L. Kaplow, "Rules versus Standards: An Economic Analysis", *Duke Law Journal* 1992, Vol. 42, p. 560. See also R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 32 (observing that the public costs of administrating rules will tend to be "front-loaded", whereas the costs of administering standards tend to be "backloaded").

[2424] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 258; L. Kaplow, "Rules versus Standards: An Economic Analysis", *l.c.*, p. 561-562; R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 25-30; B. Coene, *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, *o.c.*, p. 349-358.

[2425] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 25-26.

[2426] *Ibid*, p. 27-28.

[2427] *Ibid*, p. 28

[2428] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 259.

[2429] B.M. Hutter, *Regulation and Risk. Occupational Health and Safety on the Railways*, Oxford, Oxford University Press, 2001, p. 76.

concerns regarding unfettered discretion of enforcement officials.[2430] Conversely, rules are generally considered to provide greater legal certainty and consistency in application. When promulgating (or updating) a legal norm, lawmakers must consider the degree of precision or specificity with which they will issue their legal pronouncement. Which approach is likely to yield the best result? A rule or a standard? In the field of law and economics, a considerable body of scholarship has been developed which deals precisely with this issue. While said scholarship does not provide a definitive answer to the question of whether or not the distinction between controllers and processors should be maintained, it does provide an interesting analytical framework which merits discussion.

ii. Optimal specificity of legal rules

1203. ECONOMIC APPROACH – Scholars in the field of law and economics approach the issue of specificity of rule-making in terms of economic efficiency. They essentially ask themselves the following question: given the activity to be regulated, what is the optimal level of differentiation and precision?[2431] Ehrleich and Posner have extensively catalogued the benefits and costs associated with the promulgation of rules and standards respectively.[2432] They take into account benefits and costs not only at the moment of promulgation, but also at the moment of application (e.g., costs of interpretation, risks of over- or underinclusion).[2433] Since then, other scholars have built upon these insights and identified additional considerations that can influence the cost-benefit analysis (e.g., the degree of specialisation of decision-makers[2434]) or incorporated insights from other disciplines (e.g. behavioural analysis[2435]).[2436] It is

---

[2430] *Id.* See also R. Baldwin and M. Cave, *Understanding regulation – Theory Strategy and Practice*, o.c., p. 119 (who refer to rules as "specification" or "design" standards, whereas standards in the sense above are referred to as "performance" or "output" standards). On the benefits of principles see also N. Sethi, "Reimagining Regulatory Approaches: on the Essential Role of Principles in Health Research Regulation", *Scripted* 2015, Vol. 12, Issue 2, p. 91-116., accessible at http://script-ed.org/?p=2103 (last accessed 28 March 2016).

[2431] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 261 et seq. (who define the optimum choice as the option which maximises the excess of benefits over costs). See also B. Coene, *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, *o.c.* p. 224 et seq and 349 et seq (who argues, as regards the question of whether further specificity and differentiation is desirable, test is whether further differentiation increases likelihood of realising policy objectives, as long as the cost of differentiation does not exceed the benefits; or that optimal when the legislative measures contributes to the greatest possible realisation of the policy objective which exceeds the cost of formulation and application). See e.g. also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 6 (who consider the optimal degree of specificity of legal rules as that which maximimises the value of the law net of the fixed cost of lawmaking and the variable cost of adjudication).

[2432] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 262-271.

[2433] *Id.* Another way to think of the choice between rules and standards is as a choice regarding the extent to which a given aspect of a legal command should be resolved in advance or left to an enforcement authority to consider. (L. Kaplow, "Rules versus Standards: An Economic Analysis", *l.c.*, p. 561-562.)

[2434] V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 7 et seq.

[2435] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 44-57.

[2436] See also J. Black, "The Rise, Fall and Fate of Principles Based Regulation", *LSE Law Society and Economy Working Papers* 17/2010, 2010, 26 p. available at https://www.lse.ac.uk/collections/law/wps/WPS2010-17_Black.pdf (last accessed 29 March 2016).

beyond the scope of this thesis to evaluate each of these approaches in detail. Nevertheless, it is worth introducing the main insights they offer and to consider their potential implications for data protection law.

1204. RULES OF THUMB – Whether rules or standards yield the best outcome depends on a number of factors. A general rule of thumb, supported by several scholars, is that rules are likely to be preferable over standards if the primary behaviour (i.e. the regulated activity) is factually homogenous, stable, and occurs frequently.[2437] Standards, on the other hand, are likely to be preferable in situations where the primary behaviour is heterogeneous, evolves rapidly over time, or occurs infrequently. The underlying rationale is that the benefits of detailing a rule will be greater the more often it is applied.[2438] The cost of detailing a rule, however, is likely to be higher as the heterogeneity or complexity of the regulated activity increases.[2439] Moreover, if the social, economic or technical factors shaping the problem evolve rapidly over time, crafting detailed rules may yield insufficient return on investment.[2440] Finally, (certain) rules are more likely to create risks of over- or underinclusion than standards.[2441] Standards, on the other hand, are less likely to be affected by changes over time in the circumstances to which they are applied.[2442]

1205. LIMITATIONS – Before discussing how these rules of thumb might be applied in the context of data protection law, it is worth underlining that they do not always provide a clear-cut solution. As noted by Korobkin:

[2437] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 272-273; R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 42-43 ("*If disputes are frequent and factually homogeneous, rules are likely to have lower administrative costs, and thus are more desirable than standards on that score. If disputes are infrequent and/or factually heterogeneous, standards are preferable because they will likely be more cost effective for lawmakers to administer. Whether rules or standards have higher advice costs depends on whether the standard requires a complex investigation or merely a reference to a widely-shared social norm and the complexity of the comparable rule.*"). See also B. Coene, *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, *o.c.*, p. 359-361.

[2438] See e.g. L. Kaplow, "Rules versus Standards: An Economic Analysis", *l.c.*, p. 563.

[2439] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 274.

[2440] Von and Parisi refer to this as "the problem of obsolescence"; arguing that as the rate of obsolescence increases, the value of the legal rule decreases (V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 10)

[2441] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 42-43 "Overinclusion" refers to the situation whereby a rule prohibits or otherwise limits socially desirable behavior. Underinclusion refers to situation whereby the rule permits socially undesirable conduct (*Ibid*, p. 36) However, as Korobkin also notes, the lack of ex ante clarity associated with standards will lead to some well-intentioned undesirable behavior on the part of citizens, and errors in applying standards might cause them to be over- or underinclusive as applied (*Ibid*, p. 44). See also L. Kaplow, "Rules versus Standards: An Economic Analysis", *l.c.*, p. 565 (arguing that the suggestion that rules are more prone to over- or under-inclusiveness is misleading because typically it implicitly compares a complex standard and a relatively simple rule, whereas both rules and standards can in fact be quite simple or highly detailed in their operation).

[2442] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 277. See also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 10.

"*Although a thorough economic analysis of the comparative costs of rules and standards provides a variety of relevant insights into the ultimate choice of legal form, it provides no clear prescription for how to balance the various competing factors, some of which favour rules and others of which favour standards. Consequently, economic analysis of the choice of legal form does not provide lawmakers with a rule, even a complex one, for choosing between rules and standards in a particular factual situation.*"[2443]

iii. Implications for data protection law

1206. A MIX OF STANDARDS AND RULES – European data protection law consists of a mix of standards and rules. The principle of data accuracy, for example, promulgates a standard for determining which measures controllers should adopt to ensure data accuracy. The regulation of the relationship between controllers and processors, on the other hand, is closer to a "rule" than a standard. As soon as the relationship between two parties is qualified as a controller-processor relationship, certain specified legal results follow. Of course, not every implication (legal pronouncement) that follows from the qualification of a party as either a controller or processor is itself a rule.[2444] Nevertheless, I would argue that the differentiation between controllers and processors was introduced primarily to facilitate the promulgation of rule-like requirements (i.e., the need to ensure legal binding which contains certain minimum elements and the obligation for processors to only act on the instructions of the controller).[2445] The rule-like quality of the controller-processor model stands in stark contrast with the standard-like approach which has been developed in relation to separate and joint control. Separate controllers enjoy a considerable flexibility when allocating responsibility amongst each other, as long as "*as long as they ensure full compliance*".[2446] In case of joint control, the controllers are obliged to determine their respective responsibilities "*in a transparent manner*" and in manner which "*duly reflect[s] the joint controllers' respective effective roles and relationships vis-à-vis data subjects*".[2447]

[2443] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 43. Korobkin goes on to note that "*One view of this state of affairs is that economic reasoning has failed to resolve the question of whether lawmakers should make legal pronouncements in the form of rules or standards. Another view is that selecting a legal form is an activity more suited to being guided by a standard than by a rule.*" See also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 7 et seq (observing that each of the variables above, do not necessarily reinforce each other / can work in opposite directions)

[2444] Moreover, it should be observed that, over time, the *distinction* between controllers and processors itself has come to resemble more of a standard than a rule. The criteria to distinguish between controllers and processors are increasingly applied in a flexible and more open-ended fashion. Regulators have supplemented the statutory criteria (purpose, means, on behalf) with additional criteria (e.g., image given to data subject, level of instruction, degree of expertise), whereby none of these criteria themselves is considered determinative. As observed by Gilbert, the approach of the Working Party seems to have become a "balancing test" or "sliding scale" rather than a rigid adherence to existing criteria. Cf. *supra*; nr. 963).

[2445] The question of whether it is desirable to maintain the distinction between controllers and processors should be viewed primarily in this light.

[2446] Opinion 1/2010, *l.c.*, p. 24.

[2447] See article 26(1)-(2) GDPR.

1207. PRIMARY ACTIVITY – As a general matter, it is clear that type of activities regulated by data protection law are highly heterogeneous and evolve rapidly. Based on this observation, the use of standards might appear preferable over the use of rules.[2448] On the other hand, data processing activities are a part of daily life and occur on a massive scale. This would suggest that the promulgation of certain rules might nevertheless provide significant economies of scale. What is relevant for our current analysis, however, is not whether the primary activity regulated by data protection law *as a whole* is homogenous or heterogeneous, stable or unstable, frequent or infrequent. What is relevant is whether the *primary activity regulated by the controller-processor model* - i.e. outsourcing - is homogenous or heterogeneous, stable or unstable, frequent or infrequent.

iv. Implications for the controller-processor model

1208. OVER- AND UNDER-INCLUSION – The use cases presented in Part IV offered a small glimpse of the increasingly complex manner in which organisations collaborate, including in case of outsourcing. The cloud computing use case illustrated that there are a variety of ways in which one organisation might process personal data "on behalf of" another entity. In this context, the "rule-like" approach of the controller-processor model creates risks of both over- and under-inclusion.[2449] Hon and Millard, for example, have argued that considering all PaaS and IaaS providers as "processors" is essentially *overinclusive*, particularly in cases where the personal data processed by them is rendered unintelligible through encryption.[2450] Conversely, the argument can also be made that the controller-processor model is *underinclusive* in cases where the service providers exercise significant influence over either the purposes or means of the processing.[2451]

1209. ASSESSMENT – Overinclusion is generally considered acceptable as long as the adverse impact on socially desirable behaviour is minimal.[2452] Arguably, unnecessary

---

[2448] Regarding the desirability of detailed rules vs. general principles in data protection regulation see Home Office (Great Brittain), Computers and Privacy, Cmnd. 653, Her Majesty's Stationary Office (HMSO), London, 1975; reproduced by Home Office (Great Brittain), Report of the Committee on Data Protection, Cmnd. 7341, HMSO, London, 1978, p455-456; G. Dworkin, "The Younger Committee Report on Privacy", *l.c.*, p. 402 and F. Robben, F., "Toepassingsgebied en begripsdefinities", *l.c.*, p. 24.

[2449] Regarding the distinction between over- and underinclusion see *supra*; footnote 2441. Generally speaking, problems of overinclusion and underinclusion are more frequent the greater the heterogeneity of the conduct intended to be affected by a rule (I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 270.)

[2450] Cf. *supra*; nr. 972.

[2451] Of course, cloud providers who determine either the purposes or « essential » means of the processing are considered as (joint) controllers rather than processors, and therefore fall outside the controller-processor model all together. Nevertheless, the primary activity being regulated in such a cases is still the activity of outsourcing, which is the intended remit of controller-processor model.

[2452] Based on R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 37 ("*Rules also have lower undesirable behavior costs when the behavior deterred by an overinclusive rule is not highly valuable or when the behavior permitted by an underinclusive rule is not highly costly*"). See also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 5 (arguing that imperfections of a rule are more or less significant depending on the relative size of the value of the

transaction costs (e.g., the conclusion of controller-processor agreements in cases where its added value is minimal) is only significantly detrimental once it reaches a certain scale. From the perspective of the provider of a processing service, however, issues of overinclusion become significant once the obligations directly applicable to processors require substantial additional effort.[2453] Problems of overinclusion can be mitigated by either allowing enforcement officials to wave application of a rule in specific instances or by adding specific exceptions to the rule.[2454] The problem of underinclusion, on the other hand, can be remedied by backing the rule up with a standard.[2455] The regulatory guidance regarding joint and separate control has essentially done just this: in situations where the provider of a processing service is considered a controller rather than a processor, the parties are expected to put in place "clear and equally effective allocation of obligations and responsibilities".[2456]

1210. INTERPRETATION COSTS – In theory, rules offer greater ex ante certainty to both private actors and regulators. As soon as the fact pattern arises which triggers the application of the rule, the legal consequences of this fact pattern are already determined.[2457] From this perspective, rules have the potential to result in lower interpretation costs than standards.[2458] The controller-processor model offers a relatively clear set of rules in situations where the factual circumstances can easily be mapped to the model and its implicit assumptions regarding autonomy and control.[2459] For those cases, the model results in decreased interpretation costs for both private

---

regulate activity and the gravity of negative effects absent legal constraints). It should be noted however, that imposing a fixed model may also have hidden costs, such as deterring development of more innovative which might be more effective in practice (see R. Baldwin and M. Cave, *Understanding regulation – Theory Strategy and Practice*, o.c., p. 119 (who note that the use of detailed specification standards [rules] may inhibit innovation and the development of new, perhaps safer and more efficient modes of operation).

[2453] Cf. *infra*; nrs. 1221 et seq.

[2454] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 268: "*The problem of overinclusion is frequently dealt with by delegation to enforcement officials of authority to wave application of the rule. […] In principle one could rewrite the rule to specify all the possible exceptions; but in practice it may be cheaper to allow ad hoc exceptions to be made at the enforcement level – as recognized by even the severest critics of official discretion. Again, however, some benefits of governance by rules are sacrificed by recognizing exceptions based on implicit use of an overriding standard*".) Accommodating factually different situations can in principle also be accommodated through more detailed rules, but this will generally increase the complexity of the rule by introducing multiple exceptions and sub-rules (R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 36. As we will see later, the EU legislator has mitigated the issue of overinclusion primarily by adding exceptions (in particular by incorporating the liability exemptions of the E-Commerce Directive). Cf. *infra*; nrs. 1246 et seq.

[2455] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 268 ("*The problem of underinclusion can be solved by backing up the rule with a standard. […] The result of adding a standard is, however, to sacrifice some of the benefits of the rule.*")

[2456] Opinion 1/2010, *l.c.*, p. 24

[2457] R.B. Korobkin, "Behavioural analysis and legal form: Rules vs. Standards Revisited", *l.c.*, p. 32

[2458] Rules do not always result in lower interpretation costs than standards. For example, if a rule is very complex, it is likely to require subject-matter expertise in its interpretation. Moreover, if the application of standard is intuitive and straightforward even to laymen, a standard may still have lower interpretation costs (I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 270-271).

[2459] Regarding the implicit assumptions of autonomy and control underlying the controller-processor model see *supra*; nr. 1126.

actors and regulators. In situations where the factual circumstances do not neatly map the controller-processor model, however, the opposite is true. Interpretation costs increase as both private actors and regulators have to invest more time and resources analysing and debating the legal status of each actor. The desirability of abolishing (option A) or retaining the controller-processor model (option B) therefore depends, at least in part, on whether the model is still readily applicable in a sufficiently large number of circumstances. As noted by Ehrlich and Posner:

> "*a point is eventually reached at which the social costs generated by its imperfect fit with current reality exceed the benefits of having minimized uncertainty as to which rule would be followed.*"[2460]

1211. ASSESSMENT – Whether the interpretation costs associated with the controller-processor model have come to exceed its benefits is essentially an empirical question.[2461] It is beyond the scope of this thesis to make such an assessment. Several responses to the Commission consultation suggest that interpretation costs of the controller-processor model already exceed its benefits, but an empirical analysis would be necessary in order to make a definitive assessment (e.g. by posing this particular question to a large number and representative sample of stakeholders). It should be noted, however, that many objections concerning the controller-processor model concern the *concepts* of controller and processor, as well as the *implications* associated with these concepts, rather than the *differentiation* among parties involved in the processing of personal data as such. In fact, most stakeholders advocating in favour of abolishing the distinction between controllers and processors still advocate in favor of differentiating between parties involved in the processing and tailoring their obligations in light of their "actual role".[2462]

D. Final text GDPR

1212. OUTLINE – The final text of the GDPR retained the controller-processor model. Significant changes were introduced however, as regards the allocation of responsibility and risk. Specifically, the GDPR imposes a considerable number of obligations directly upon processors and renders them liable in case of violations.

[2460] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 278. The authors make this point in relation to the rule of "stare decisis" (which requires courts to adhere to precedent), but in my view similar point can be made in relation to the controller processor model, which is essentially a codification of past regulatory guidance regarding appropriate measures in case of outsourcing.

[2461] See also V. Fon and F. Parisi, "Codifications and the optimal specificity of legal rules", *l.c.*, p. 10-11, who refer to this as the "obsolescence problem" and discusses its relationship to economies of scale in adjudication.

[2462] Cf. *supra*; nrs. 1175 et seq. By definition, this implies differentiation among the actors involved in the processing, even if concepts of "controller" and "processor" were themselves to be abolished.

1213. OBLIGATIONS FOR PROCESSORS – Under the GDPR, processors are obliged to ensure confidentiality and security of processing, independently of the existence of a contractual arrangement to that extent between controllers and processors (article 30). Processors are also obliged to maintain appropriate records of all processing activities which they carry out on behalf of a controller, and to present such records to supervisory authority at request (article 28-29). Processors must also designate a data protection officer in the same cases where this is required from controllers (article 35). Restrictions regarding international transfers now also apply directly to processors (article 40). Finally, it is also envisaged that codes of conduct and certification mechanisms be developed for processors (articles 38-39).

1214. DATA PROTECTION BY DESIGN – The EU legislature chose not to assimilate controllers and processors as regards the obligation of data protection by design.[2463] This is regrettable, given substantial influence processors have in determining the means of the processing. In my view, it would have been reasonable to impose a similar obligation upon processors, as long as one takes into account the intended purpose of the services they offer.[2464]

1215. LIABILITY MODEL – Article 77 GDPR provides that any controller and processor involved in the processing shall be liable for the damage caused by the processing which is not in compliance with the GDPR. The processor, however, shall only be liable only if he failed to comply with the obligations of the GDPR directed specifically to processors or if he acted outside or contrary to lawful instructions of the controller (article 77(2)). Article 77 GDPR is conceptually similar to the "combined approach" described earlier (general and proportional liability).[2465] The main difference is that the GDPR retained both the concepts of controller and processor in order to further differentiate among the obligations incumbent upon each party involved in the processing.

1216. ESCAPE CLAUSE – Article 77(3) provides that a controller or processor may be exempted from liability provided it proves that it is not in any way responsible for the event giving rise to the damage. This provision echoes article 23(2) of Directive 95/46, with the important difference that its scope of application now also extends to

---

[2463] Article 23 provides that "*having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*"

[2464] See also Microsoft, "Protecting Data and Privacy in the Cloud", *Reactive Security Communications*, 2014, p. 3-5 (arguing that it is responsibility of cloud providers to design services in such a way that enables compliance).

[2465] Cf. *supra*; nrs. 1190 et seq. For a discussion of the ratio legis underlying this provision see also supra; nr. 587.

processors.[2466] Another change is the introduction of the words "in any way", which clarifies that faults contributing indirectly to the damage may still constitute grounds for liability. At the end of the day, however, the liability regime contained in the GDPR is still essentially a fault-based regime as regards privacy and data protection breaches, albeit with a reversed burden of proof.[2467]

1217. RISKS OF UNDER- AND OVERINCLUSION? – Despite the changes made in relation to the obligations incumbent upon processors, the controller-model is still not able to accommodate all forms of outsourcing. The risk of *underinclusion* has been addressed – in part – by addressing the implications of joint control.[2468] As will be seen in the next section, the GDPR has essentially codified the standard put forward by the Article 29 Working Party in Opinion 1/2010. The GDPR does not, however, explicitly address the situation of collaborating single controllers. In other words, the GDPR may still be underinclusive in practice in relation to situations of separate control.[2469] Risks resulting from *overinclusion* have arguably become more significant now that processors are directly subject to certain obligations. The incorporation of the liability exemptions of the E-Commerce Directive (cf. *infra*) significantly mitigates the risks of overinclusion. Nevertheless, there may still be service providers whose services do not neatly map to the exemptions, which may result in overinclusion in specific instances.

1218. EVALUATION – Every legal norm, whether it be a standard or a rule, is imperfect in the sense that it cannot operate without costs.[2470] Rules are attempts to model and rationalize human behavior, and every form of rationalization implies a certain loss.[2471] Especially in highly dynamic environments, there will always be cases where the regulatory paradigms and concepts which underlie rules do not neatly map reality or lead to suboptimal outcomes.[2472] On the other hand, complexity does not justify inaction. As noted by Schmidtchen

---

[2466] For an analysis of the escape clause contained in article 23(2) of Directive 95/46 see *supra*; nrs. 125 et seq.

[2467] P. Larouche, M. Peitz and N. Purtova, *Consumer privacy in network industries – A CERRE Policy Report*, Centre on Regulation in Europe, 25 January 2016, p. 58, available at http://cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf (last accessed 25 March 2016) The only exception of course is in cases where the GDPR imposes an obligation of result.

[2468] See also *infra*; nr. 1224.

[2469] Regarding the diffference between joint control, partial joint control and separate control see *supra*; nrs. 107 et seq.

[2470] D. Schmidtchen a.o., "The Internalisation of External Costs in Transport: From the Polluter Pays to the Cheapest Cost Avoider Principle", *l.c.*, p. 111.

[2471] Id. ("*all institutions – here broadly understood as rules and norms – are imperfect in the sense that they do not operate without costs: opportunity costs in terms of a misallocation of resources and risks, setup and operating costs. Consequently, rationality requires taking all costs into account when making an institutional choice*".)

[2472] See also I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 268 "*Greater specificity of legal obligation generates allocative inefficiency as a result of the necessarily imperfect fit between the coverage of a rule and the conduct sought to be regulated [...] The inherent ambiguity of language and the limitations of human foresight and knowledge limit the practical ability of the rule maker*

> "*Human behaviour is complex and not always easy to predict. However, if one seeks to make problems tractable enough to provide for some illumination, we need to make simplifying assumptions which do not capture reality. The optimal scale of a map depends on the context that is going to be used in; a map with a scale of 1:1 is clearly of no use at all. The same applies to modelling human behaviour.*"[2473]

On balance, the desirability of abolishing or retaining the controller-processor model is a question of the optimal degree of differentiation and specificity of legal norms. Determining optimality is an extremely complicated exercise, as it requires balancing the costs and benefits of many different variables. Obtaining an accurate and detailed picture of each of these variables is extremely difficult in practice.[2474] In practice, the approach adopted by legislatures may not be a purely rational choice, but rather the result of lengthy rounds of negotiation and revision, compromise and accommodation.[2475] In the GDPR, the EU legislature decided to retain the controller-processor model. It also provided greater recognition to situations of joint control, to clarify that the controller-processor model is by no means the only model of collaboration. Finally, by imposing additional obligations directly upon processors, the GDPR at least partially alleviates some of the systemic issues which previously plagued the controller processor-model. Taken together, this is likely to be an adequate approach, at least for the time being. In the long term, however, it may become necessary to revisit the current approach. Chapter 4 will therefore outline an alternative approach, which omits the problematic concepts of controller and processor, while supporting differentiation and greater flexibility in terms of the allocation of responsibility and risk.[2476]

4 SYSTEMIC

1219. PREFACE – Systemic solutions are solutions that involve modifying the implications associated with the controller and processor concepts. The point of departure is that certain functions fulfilled by the controller and processor concepts within the regulatory scheme of Directive 95/46 can give rise to unintended or undesirable consequences in practice. Systemic solutions seek to address these issues by adjusting the function of the controller and processor concepts in relation to one or more provisions.

---

to catalog accurately and exhaustively the circumstances that should activate the general standard. Hence the reduction of a standard to a set of rules must in practice create both overinclusion and underinclusion"

[2473] D. Schmidtchen a.o., "The Internalisation of External Costs in Transport: From the Polluter Pays to the Cheapest Cost Avoider Principle", *l.c.*, p. 118

[2474] R. Baldwin and M. Cave, *Understanding regulation – Theory Strategy and Practice*, o.c., p. 122-124. See also B. Coene, *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, *o.c.*, p. 232 et seq.

[2475] *Ibid*, p. 124

[2476] Cf. *infra*; nrs. 1257 et seq.

1220. OUTLINE - Proposed systemic measures include:

(1) associating the same or similar legal consequences to both the controller and processor concepts (partial assimilation);

(2) providing greater recognition of situations of joint control;

(3) using alternative means of securing transparency and accommodation of data subject rights;

(4) use of standards to determine the scope of obligations incumbent upon each party involved in the processing; and

(5) enhancing the degree of contractual flexibility in the relationship between controllers and processors.

4.1 PARTIAL ASSIMILATION

1221. PROPOSAL – Under Directive 95/46, the legal status of a party as controller or processor has significant ramifications.[2477] First, it may have a determinative influence on whether EU law applies to the processing at all. Second, it also determines whether, and if so, to what extent the party shall be accountable towards regulators and data subjects. In its draft proposal for the GDPR, the Commission reduced the systemic importance of the distinction in several ways. First, it provided that the territorial scope of EU law would no longer be dependent on controller or processor status. Second, it made processors directly accountable to regulators and data subjects for those aspects of the processing for which they are responsible. Finally, it rendered a substantial number of provisions directly applicable to processors.[2478] The following table provides a comparative overview of the main changes introduced by the EC draft proposal:

Relevant provisions	**Directive 95/46**		**EC Draft GDPR**	
	Controllers	Processors	Controllers	Processors
Applicable law	✓	X	✓	✓
Principles of data quality	✓	X	✓	X
Legitimacy of processing	Implied	X	Implied	X
Sensitive data	Implied	X	Implied	X
Transparency	✓	X	✓	X
Data subject rights	✓	X	✓	Applicable through contract (with exceptions)
Co-operation with supervisory authority	Implied	Implied	✓	✓
Data protection by design and by default	Implied	X	✓	X

[2477] Cf. *supra*; nrs. 188 et seq.
[2478] See also *supra*; nr. 533.

Documentation	Implied	Not specified	✓	✓
Confidentiality	✓	✓	✓	✓
Security	✓	Applicable through contract	✓	✓
Data breach notification[2479]	X	X	✓	✓
DPIA, prior authorization	✓	X	✓	✓
Data protection officers	✓	X	✓	✓
Codes of conduct, certification	✓	Not specified	✓	✓
International transfers	✓	Not Specified	✓	✓
Liability	✓	X	✓	✓
Administrative fines	Implied	Not Specified	✓	✓

Table 2 Comparison Directive 95/46 – EC proposal GDPR[2480]

1222. RATIONALE – As indicated earlier, the stated objective of the European Commission was to "clarify and detail" the responsibilities and liability of controllers and processors with a view of establishing legal certainty.[2481] Be that as it may, by imposing the same or similar legal consequences to the legal status of both controller and processor, the Commission proposal also reduced the systemic importance of the distinction.

1223. COUNTERARGUMENTS – As indicated earlier, certain commentators felt that by imposing the same or similar obligations directly upon processors, there may be a risk of confusion as to who is ultimately responsible for ensuring compliance.[2482]

4.2 GREATER RECOGNITION OF JOINT CONTROL

1224. PROPOSAL – In its draft proposal for the GDPR, the Commission introduced a provision requiring joint controllers to determine their respective responsibilities for compliance, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.[2483] In addition,

[2479] As regards the obligation to notify data breaches, a distinction should be made between the obligation to inform breaches to the controller and the obligation to notify breaches to supervisory authorities and data subjects. Only the controller is obliged to notify the data subject and supervisory authorities. The processor is only obliged to notify the controller.
[2480] Legend: a check mark (✓) indicates that the provision in question is directly and expressly applicable to the actor in question; an "X" indicates that it is clear that the provision in question does not directly apply to the actor in question. The color red signals that the final text of the GDPR introduced a change in relation to Directive 95/46. The color green signal that the final text of the GDPR differs from the original EC proposal with respect to the scope of applicability of this provision.
[2481] Cf. *supra*; nr. 1180.
[2482] Cf. *supra*; nr. 1181.
[2483] Cf. *supra*; nr. 535.

the proposal also stipulated that in situations where more than one controller is involved in the processing, each controller shall be jointly and severable liable for the damages as a whole.

1225. RATIONALE – While Directive 95/46 already recognised the possibility of joint control, it did not spell out its legal implications. The absence of guidance by the EU legislature led to uncertainty and divergent opinions in practice.[2484] Providing greater recognition of joint control signals more clearly that the controller-processor model is by no means the only manner in which parties involved in the processing of personal data can structure their collaboration. It also provides more stable legal footing for parties who choose to do so, thereby increasing legal certainty.

1226. COUNTERARGUMENTS – The main counterargument against the proposal put forward by the European Commission is that it provides only a partial solution. In practice, not every collaboration between controllers takes the form of joint control.[2485] There may, however, also be situations in which a collaboration between separate controllers requires a mutual arrangement to ensure implementation of adequate data protection safeguards, not least as regards transparency of processing and the exercise of data subject rights. This issue will be elaborated further under the next subsection.

4.3 "NO WRONG DOOR" AND "SINGLE POINT OF CONTACT"

1227. PROPOSAL – The General Approach of the Council provided that in case of joint control, joint controllers should in principle designate among themselves a *single point of contact* for data subjects to exercise their rights.[2486] Irrespective of such an arrangement, however, the data subject would still be able to exercise his or her rights in respect of and against each of the joint controllers ("*no wrong door*").[2487]

1228. RATIONALE – The introductory text accompanying the General Approach did not specify why the Council imposed the obligation to provide for a single point of contact, combined with a "no wrong door" policy. One might speculate, however, that the proposal was motivated by the finding that the processing of personal data may involve an increasing number of controllers. The multiplication of controllers involved in the processing can make it difficult for data subjects to know who to turn to in order to exercise their rights. By providing that joint controllers should put in place a single point of contact, the data subject is relieved from the burden of determining who is

[2484] See also European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", *l.c.*, p. 5 ("*This is not helped by the fact that the concept of joint controller is not well acknowledged by European data protection law and supervisory authorities.*")
[2485] Cf. *supra*; nrs. 101 et seq.
[2486] See article 24(1) of the General Approach. Under the General Approach, joint controllers would be exempted from this obligation in cases where the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.
[2487] Article 24(2) of the General Approach.

responsible for which aspect of the processing. By further stipulating that the data subject is able to exercise his or her rights against each of the joint controllers, the data subject retains maximum recourse avenues in case of harm.

1229. COUNTERARGUMENTS – The main reproach one could make against the proposal of the Council is the same as the one articulated under the previous section, i.e. that it provides only a partial solution. It does not address the case where the processing involves a large number of collaborating single controllers (i.e., "separate controllers" or "controllers in common"). Moreover, in case of joint control, data subjects were already in a position to exercise their rights in full vis-à-vis every joint controller involved in the processing.[2488] From this perspective, one could argue that the "no wrong door" policy did not really add anything new.

4.4 TAILORING OBLIGATIONS

1230. PROPOSAL – A proposal which has not yet been put forward is to introduce language which would allow adjudicators to further tailor the obligations of controllers and/or processors in light of their specific role in the processing. One way to do this would be to codify the language used by the Court of Justice in *Google Spain* to indicate the limits of the obligations incumbent upon search engines ("*within the framework of its responsibilities, powers and capabilities*"[2489]). An alternative formulation can be found in the OECD Recommendation on Digital Security Risk Management. The second principle ("responsibility") stipulates that all stakeholders should take responsibility for the management of digital security risks "*based on their roles, the context and their ability to act*".[2490]

1231. RATIONALE – The precise scope of data protection obligations must always be assessed in context. A party's obligations might indeed be lighter - or more onerous -

[2488] In case of joint control, each joint controller is in principle responsible and liable for the processing as a whole. As a result, the data subject should already be able to exercise his rights vis-à-vis any of the (joint) controllers involved in the processing. Even if the specific controller approached by the data subject is not internally responsible for that element of the processing, he remains accountable as joint controller for operations performed by his fellow joint controllers (or processors). See also *supra*; nr. 145.
[2489] Judgement in *Google Spain*, C-131/12, EU:C:2014:317, paragraph 38. See also supra; nr. 1066 et seq.
[2490] See the second principle of the OECD, Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2015, accessible at http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf. Such language could be introduced either after the specific provision in question (e.g., by specifying that *"it shall be for the controller [and/or processor] to ensure that paragraph 1 is complied with, taking into account its responsibilities, powers and capabilities [alternative: taking into account context role and ability to act]"*), or when determining the scope of liability exposure (e.g., by specifying that "*any party who has contributed to the harm suffered may be exempted from liability insofar as it has implemented every reasonable measure to prevent and remove harm, taking into account its responsibilities, powers and capabilities [alternative: taking into account context role and ability to act]*)".

depending on the purposes pursued by the processing and the risks for data subjects.[2491] Certain provisions of Directive 95/46 fail to provide adequate flexibility in all contexts.[2492] By incorporating additional standards into the legal framework, it may be possible to soften the adverse impact of certain rule-like ("all or nothing") features of the current framework.[2493] On the one hand, it would enable adjudicators limit the scope of a party's obligations in cases where ensuring compliance of certain aspects (or for certain stages) of the processing is beyond its actual control capabilities.[2494] On the other hand, it would enable adjudicators to impose heightened responsibilities on other actors where this is reasonable in light of their role, even if the processing at issue does not strictly reside within their sphere of "control".[2495]

1232. COUNTERARGUMENTS – Introducing standards to mitigate the adverse consequences of rules implies sacrificing some of the benefits which rules otherwise provide.[2496] While introducing a standard may enhance flexibility and adaptability, it is likely to increase the interpretation and administration costs in situations where this would otherwise not be necessary (i.e., where simple application of the rule would lead to the socially desirable outcome). Moreover, the argument can be made that most of the provisions of Directive 95/46 do already allow for flexibility in their application.[2497] As a

---

[2491] B. Van Alsenoy, A. Kuczerawy and J. Ausloos, "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *l.c.*, p. 44. See also Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, *l.c.*, p. 59-60.

[2492] For example, the restrictions regarding sensitive data in the context of processing of personal data by search engines. Cf. *supra*; nr. 1068.

[2493] Cf. *supra*; nr. 1138. It should be noted, however, that by imposing additional obligations directly on processors, the differentiation between controllers and processors becomes less stark (less of an "all or nothing" exercise).

[2494] Cf. *supra*; nrs. 1138 et seq.

[2495] See also *supra*; nr. 881. See also the critique of Ruggie regarding use of concept of "control" to delineate responsibilities (J. Ruggie, "Clarifying the Concepts of "Sphere of influence" and "Complicity"", Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, A/HRC/8/16, 15 May 2008, at paragraphs 16-17, available at http://198.170.85.29/Ruggie-companion-report-15-May-2008.pdf (last accessed 4 May 2016). Ruggie explicitly discards the use of concepts of "control" and "causation" as means to assign responsibility: "*Furthermore, the concepts of control or causation could wrongly limit the baseline responsibility of companies to respect rights. The responsibility to respect requires that companies exercise due diligence to identify, prevent and address adverse human rights impacts related to their activities. If the scope of due diligence were defined by control and causation this could imply, for example, that companies were not required to consider the human rights impacts of suppliers they do not legally control, or situations where their own actions might not directly cause harm but indirectly contribute to abuse.*" Ruggie goes on to posits alternative model of "due diligence" and complicity, which requires "a process whereby companies not only ensure compliance with national laws but also manage the risk of human rights harm with a view to avoiding it. *The scope of human rights related due diligence is determined by the context in which a company is operating, its activities, and the relationships associated with those activities.*"

[2496] I. Ehrleich and R. A. Posner, "An Economic Analysis of Legal Rulemaking", *l.c.*, p. 268 ("*The problem of underinclusion can be solved by backing up the rule with a standard. […] The result of adding a standard is, however, to sacrifice some of the benefits of the rule.*")

[2497] See also Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", *l.c.*, p. 4-5 ("*Even where processing of personal data within the scope of the Directive is involved, not all the rules contained therein may be applicable in the particular case. A number of provisions of the Directive contain a substantial degree of flexibility, so as to strike the appropriate balance between protection of the*

result, flexibility should only be enhanced where needed, which may also be achieved by adding exceptions as opposed to a general standard. This could be done either by introducing (blanket) exemptions for certain types of processing activities (e.g., by incorporating the liability exemptions contained in the E-Commerce Directive[2498]), or by adding (more limited) exceptions to specific provisions. Finally, as illustrated by the jurisprudence of the Court of Justice and guidance of the Article 29 Working Party, the adverse effects caused by the strict application of rules can also be softened when interpreting them.[2499]

4.5 CONTRACTUAL FLEXIBILITY

1233. PROPOSAL – Another possible measure, which is similar in nature (but more narrow in scope) than the previous one, is to enhance the degree of contractual flexibility in the relationship between controllers and processors. Specifically, rather than prescribe mandatory elements which must be included in every contract between controllers and processors, one could simply require controllers to "adduce adequate safeguards" when outsourcing personal data processing.[2500]

1234. RATIONALE – The main argument in favour of enhancing contractual flexibility is to remedy situations in which the controller-processor template is ill-suited to govern a particular outsourcing arrangement. Hon and Millard, for example, have argued that there are situations in which considering certain cloud providers as processors is excessive (e.g., in cases where the cloud provider has neither knowledge nor control of the fact that his services are used to process personal data).[2501] An additional argument, put forward by Moerel, is non-discrimination: if joint controllers enjoy full flexibility in mutually allocating responsibility, so should controllers and processors.[2502]

---

data subject's rights on the one side, and on the other side the legitimate interests of data controllers, third parties and the public interest which may be present.") See also *supra*; nr. 1066.

[2498] This approach has been advocated by Sartor and will be discussed later on. Cf. *infra*; nr. 1246.

[2499] See also *supra*; nr. 1067. Critics of this approach argue that this approach fails to provide adequate guidance for practitioners: cf. *supra*; nr. 1068.

[2500] This approach could be applied in conjunction with abolishing the distinction between controllers and processors (cf. *supra*; nrs. 1175 et seq.) and would closely resemble the approach of the Canadian Privacy Act (PIPEDA), which simply requires responsible organisations to take all reasonable steps to protect personal information under their control, regardless of where it is processed. See B. Van Alsenoy, "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *l.c.*, p. 41-42.

[2501] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 27-28. See also *supra*; nr. 1209.

[2502] L. Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, *o.c.*, p. 218 ("*I agree that the imposing of direct obligations on processors is a good way to ensure that processors in complex processing operations do not "hide" behind their processorship in order to avoid liability. However, if the Proposed Regulation allows joint controllers to divide responsibilities between them, I do not see why this possibility would not be extended to a division of responsibilities between joint processors (or between main and sub-processors) ad further between (joint) controllers and such (joint or sub-) processors. If individuals keep their rights against any of them, there seems little to be said against such possibility to divide responsibilities.*")

1235. COUNTERARGUMENTS – A first argument in favour of prescribing which elements should at a minimum be included in the contract between controllers and processors is that those elements in fact operate as "contractual safeguards" of the controller-processor relationship.[2503] By introducing these elements, the parties actually define their mutual relationship in such a way that corresponds with the controller-processor model. An additional argument is that the controller-processor model is in fact a normative construct, from which parties should not have the ability to derogate freely.[2504]

4.6 ASSESSMENT

1236. INTERNAL COMPARISON – The solutions outlined over the previous sections are by no means mutually exclusive. Each of them can be used to reduce the systemic role of the distinction between controllers and processors. Of course, substantial differences will remain, which may continue to shape the interpretation of these concepts. By assimilating the systemic role of each concept as much as possible, however, the risk can be minimised. Providing greater recognition of joint control acts in a complementary fashion. Directive 95/46 placed substantial emphasis on the regulation of controller-processor relationships, but did not address the implications of joint control.[2505] The absence of recognition and attendant uncertainty may have made this model less appealing to practitioners.

1237. INTERDEPENDENCIES – The partial assimilation of the role of controllers and processors, as well as the decision to provide greater recognition of joint control, alleviates the teleological issues regarding continuous protection and legal certainty. By imposing similar obligations upon controllers and processors, processors can be made directly accountable towards regulators and data subjects. By providing greater recognition of joint control, greater legal certainty is provided for actors whose collaboration does not neatly map with the controller-processor model. The grammatical and historical issues are not affected by the systemic solutions presented here.

[2503] See also Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", *l.c.*, p. 12. Cf. *supra*; nr. 949.

[2504] See also *supra*; nr. 1183.

[2505] The Directive has devoted very limited text to the relationship among co-controllers, and none at all to the implications of their collaboration in terms of responsibility allocation and liability. In fact, the only language in Directive 95/46/EC explicitly acknowledging the possibility of joint control towards the same processing is the passage "alone or jointly with others" in article 2(d). Granted, the choice to primarily refer to a controller in the singular may have been an editorial one (to avoid having to repeat the words "or controllers" each time the word "controller" is used). The text may even have been drafted this way to emphasize the fact that when multiple entities jointly determine the purposes and means of the processing, they in principle share the responsibility of ensuring compliance. Be that as it may, the seemingly "monolithic" concept of controller embodied by the Directive may also explain why practitioners have experienced such difficulty in assigning controllership in practice when different organisations collaborate.

1238. FINAL TEXT GDPR – For the most part, the proposal of the European Commission to partially assimilate the functions fulfilled by the controller and processor concepts was retained in the final text of the GDPR. One notable difference concerns the removal of the reference to processors in the provisions regarding data protection impact assessments and prior authorisation.[2506] The final text of the GDPR also elaborates upon the implications of joint control, but does not specifically address the implications of separate control.

1239. POSSIBLE REMEDY – The situation of separate control is less straightforward than the situation of joint control. In case of separate control, each controller pursues his own distinct purpose(s) in processing personal data.[2507] Separate controllers shall in principle only be accountable for those processing activities which are effectively under their control. As a result, they have no formal obligation to accommodate data subject rights in relation to those stages or aspects of the processing which are under the exclusive control of another party. In situations where a large number of separate controllers are involved, the risk of lack of transparency towards data subjects increases. A possible mitigation strategy could be to also require separate controllers to designate a single point of contact and implement a "no wrong door" policy, in cases where this is necessary in order to ensure fairness of processing. Interpreting the principle of fairness in this way would allow for a case-by-case assessment as to whether such a measure is necessary in light of the circumstances.[2508]

1240. STANDARDS VS. RULES – The proposals regarding the tailoring of obligations and contractual flexibility are related to the question of the optimal degree of specificity of data protection norms. The use cases analysed in Part IV illustrated that there are situations in which it is necessary to support greater flexibility in the application of controller obligations. The incorporation of standards, either as complements or replacements to rules, may help to achieve this.[2509] Other approaches are also possible, however, such as the adding of specific exceptions or the use of blanket exemptions. The optimal approach will depend on whether one considers that the adding of rules will be sufficient to stand the test of time, or that instead standards are needed to ensure adequate flexibility and adaptability. Similar considerations apply in relation to the

[2506] Contrary to the initial proposal put forward by the European Commission, the final version of the GDPR does not render these provisions directly applicable to processors.
[2507] Cf. *supra*; nr. 104.
[2508] The requirement to implement such a policy may depend on an appreciation of the facts of the case, including the image given to data subjects. Not every set of processing activities involving collaborating single controllers would require putting in place a "no wrong door policy". Take for example an online purchase. The average data subject is likely able to discern the distinction between processing activities for which the merchant acts as controller and those for which the card provider and/or payment service provider acts as controller. In such situations, the data subject may be expected to approach each controller separately for those processing activities which clearly belong to the sphere of control for either party.
[2509] See also *supra*; nr. 1209.

proposal to allow for greater contractual flexibility in the relationship between controllers and processors.[2510]

5 HISTORICAL

1241. OUTLINE – Historical solutions are solutions which seek to limit the scope of application of the controller and processor concepts to the actors and situations for which they were created. The point of departure is that the application of the controller and processor to circumstances unanticipated by the European legislature leads to unintended or undesirable consequences, at least in certain situations. Proposed solutions include (1) expanding the scope of the personal use exemption and (2) incorporating the liability exemptions contained in the E-Commerce Directive.

5.1 PERSONAL USE EXEMPTION

1242. PROPOSAL – In February of 2013, the Article 29 Working Party issued a Statement on the "current discussions" surrounding the data protection reform. The

[2510] It should be noted that the final text of the GDPR has substantially increased the number of elements to be included in the contracts between controllers and processors. Specifically, article 26(2) provides that the carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall:
(a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
(c) take all measures required pursuant to Article 30;
(d) respect the conditions referred to in paragraphs 1a and 2a for enlisting another processor;
(e) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34 taking into account the nature of processing and the information available to the processor;
(g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data; make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.

second annex accompanying the Statement concerned the future of the personal use exemption.[2511] In the Statement, the Working Party considered that

> "*the current Directive's approach to personal or household processing has an unrealistically narrow scope that no longer reflects individuals' capacity to process data for personal and household activities and has therefore become anachronistic*."[2512]

To remedy this issue, the Working Party proposed using the following five criteria to determine whether or not the personal use exemption applies:[2513]

(1) *Publicity*: is the data disseminated to an indefinite number of persons or to a limited community of friends, family members or acquaintances?

(2) *Data subjects involved* is the data about individuals who have a personal or household relationship with the person posting it?

(3) *Scale and frequency*: does the scale and frequency of the processing suggest a professional or full-time activity?

(4) *Concerted action*: is the individual acting alone or is there evidence of individuals acting together in a collective and organized manner?

(5) *Adverse impact*: what is the potential adverse impact on individuals, including intrusion in their privacy?

None of these criteria would, by themselves, necessarily exclude application of the personal use exemption.[2514] Instead, one should look at them in combination to determine whether, on the whole, the personal use exemption applies.[2515] The proposed criteria would afford data protection authorities a certain degree of discretion when deciding whether or not to take action against a particular processing activity. At the same time, using the identified criteria would promote objectivity in this decision-making process.[2516]

1243. VARIATIONS – The Article 29 Working Party proposed introducing the criteria above by way of a recital, without substantively modifying the actual language of the personal use exemption.[2517] The General Approach of the Council, however, suggested to

---

[2511] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", 27 February 2013, p. 2, accessible at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf (last accessed 16 February 2015).
[2512] *Ibid*, p. 2.
[2513] *Ibid*, p. 4.
[2514] *Id.*
[2515] *Id.*
[2516] *Id.*
[2517] *Ibid*, p. 10. The only change proposed by the Article 29 Working Party would be to change the word "purely" by the word "exclusively".

go further by omitting the word "purely".[2518] Earlier proposals made by the European Commission focused on introducing negative criteria, using phrases such as "without any gainful interest" and "thus without any connection with a professional or commercial activity".[2519]

1244. RATIONALE – The proposal of the Article 29 Working was motivated by a historical interpretation of the personal use exemption: at the time the exemption was conceived, the processing capabilities of individuals where much more limited. With the rise of Internet connectivity, new forms of communication and social interaction have emerged:

> "*[A]ccess to the internet – uncommon for natural persons in the mid 1990's – and more functional information and communications technology (ICT) has opened the way for a range of personal processing activities that the current Directive could not have been expected to anticipate.*"[2520]

The justification of the Article 29 Working Party may be complemented with the arguments advanced by scholars who have also advocated in favour of revising the personal use exemption. Garrie a.o., for example, have argued that it would be very burdensome and unrealistic to apply several of the provisions of Directive 95/46 to private individuals.[2521] Wong and Savirimuthu point out that it may be impossible for supervisory authorities to secure compliance in relation to private individuals.[2522] Finally, it has also been suggested that any attempts to do so might itself constitute an interference with individuals' fundamental right to privacy.[2523]

[2518] See Council for the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 11 June 2015, 2012/0011 (COD), 9565/15, p. 76

[2519] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, *l.c.*, p. 40. The Commission proposals were rejected, however, by both the Article 29 Working Party and the legislative bodies.

[2520] *Ibid*, p. 2 See also OECD, "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *l.c.*, p. 20-21 and 27-28and also N. Xanthoulis, "Negotiating the EU Data Protection Reform: Reflections on the Household Exemption", in A. B. Sideridis a.o. (eds.), *E-Democracy, Security, Privacy and Trust in a Digital World*, 5th International Conference, E-Democracy 2013, Springer, Communications in Computer and Information Science, 2014, p. 138.

[2521] D.B. Garrie, M. Duffy-Lewis, R. Wong and R.L. Gillespie, "Data Protection: the Challenges Facing Social Networking", *l.c.*, 131 et seq. and p. 149. See also N. Helberger and J. Van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *l.c.*, p. 104; P. Roth, "Data Protection Meets Web 2.0 – Two Ships Passing in the Night", *UNSW Law Journal* 2010, Vol. 33, p. 534 and 560 and J. Zittrain, *The Future of the Internet— And How to Stop It*, *o.c.*, p. 221, ("*[...] the sorts of administrative burdens we can reasonably place on established firms exceed those we can place on individuals--at some point, the burden of compliance becomes so great that the administrative burdens are tantamount to an outright ban*.")

[2522] R. Wong and J. Savirimuthu, "All or nothing: this is the question? The application of Art. 3(2) data protection directive 95/46/EC to the internet". *l.c.*, p. 244. See also N. Xanthoulis, "Negotiating the EU Data Protection Reform: Reflections on the Household Exemption", *l.c.*, p. 138.

[2523] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.,* p. 3 ("*It is certainly the case that an inappropriate level of scrutiny*

1245. COUNTERARGUMENTS – Data protection advocates are cautious when it comes to expanding the notion of "personal use". For all its benefits, the widespread availability of ICTs also enables individuals to inflict considerable privacy harms. Outing a sexual preference[2524], broadcasting a traumatic experience[2525], public shaming[2526] or posting "revenge porn"[2527] are all just a few clicks away. While traditional civil law remedies (e.g., defamation, breach of confidence, right to control the use of one's image, misuse of private information) may offer a solution, certain remedies show limitations when applied to the online context.[2528] Data protection laws could provide an important legal backstop in such cases. Perhaps a more compelling argument against extending the scope of the personal use exemption concerns the potential role of data protection authorities. Directive 95/46 requires Member States to provide an independent supervisory authority which is dedicated to monitoring compliance.[2529] It also stipulates that every individual should have the right to file a complaint if they feel their rights and freedoms are being harmed by personal data processing.[2530] From the perspective of an aggrieved individual, filing a complaint with a national DPA constitutes a much lower threshold than the initiation of formal legal proceedings. While the former can often be done online, free of charge, the latter is likely to entail considerable legal expense.

5.2 LIABILITY EXEMPTIONS OF THE E-COMMERCE DIRECTIVE

1246. PROPOSAL – Article 1(5)b of the E-Commerce Directive excludes from its scope *"questions relating to information society services covered by Directive 95/46* […]".[2531] A literal reading of article 1(5)b suggests that the liability exemptions provided by the E-Commerce Directive should not be applied in cases concerning the liability of

---

and regulation of natural persons' personal or household processing activities by DPAs could inhibit individuals' freedom of speech and could in itself constitute a breach of the individual's right to privacy.") . See also J. Zittrain, o.c., p. 222; R. Wong and J. Savirimuthu, "All or nothing: this is the question? The application of Art. 3(2) data protection directive 95/46/EC to the internet". *L.c.*, p. 244 and N. Xanthoulis, "Negotiating the EU Data Protection Reform: Reflections on the Household Exemption", l.c., p. 138.

[2524] See e.g. High Court of Justice, *Applause Store Productions Limited and Matthew Firsht v. Grant Raphael*, 24 July 2008, [2008] EWHC 1781 (QB), accessible at www.bailii.org.

[2525] See e.g. Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14, accessible at available at www.dirittoegiustizia.it

[2526] High Court of Justice, Stephen Robins and Gabbitas Robins v. Rick Kordowski and Tim Smee, 22 July 2011, [2011] EWHC 1912 (QB), accessible at www.bailii.org.

[2527] See http://www.endrevengeporn.org/.

[2528] See e.g. D. Erdos, "Filling Defamation's Gaps: Data Protection and the Right to Reputation", *Oxford Legal Studies Research Paper* 2013, No. 69, available at https://www.repository.cam.ac.uk/bitstream/handle/1810/245805/OA1491_Reputation%20and%20Data%20Protection%20Article_Final_title.pdf?sequence=4 (last accessed 17 January 2015).

[2529] Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", *l.c.*, p. 1

[2530] *Ibid*, p. 3.

[2531] Article 1(5)b of Directive 2000/31.

"controllers" or "processors", as these matters are regulated by Directive 95/46.[2532] Several scholars have advocated against such an outcome, arguing that the liability exemptions of the E-Commerce Directive should also be applied in matters concerning data protection.[2533] In its draft proposal for the GDPR, the European Commission incorporated the intermediary liability exemptions contained in the E-Commerce Directive by way of article 3(3).[2534]

1247. RATIONALE – The European Commission did not motivate its proposal to incorporate the liability exemptions for internet intermediaries. Scholars who advocated in favour of applying the liability exemptions of the E-Commerce Directive have advanced different reasons. Hon and Millard, for example, simply argued that it would be "appropriate" or "justified" to do so in cases where the provider of a (cloud-based) processing service has no knowledge or control over the processing of personal data.[2535] In support of their argument, they also invoke considerations of non-discrimination.[2536] Sartor, on the other hand, mainly argued in favour of applying the exemptions to avoid otherwise unreasonable outcomes in relation to the dissemination of content via the Internet[2537] and to ensure a uniform approach as regards the liability of internet service providers.[2538]

[2532] Contra: G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law*, 2014, Vol. 21, No. 3, p. 574 ("*[Article 1(5)b of the eCommerce Directive] has sometimes been read as excluding violations of data protection from the e-commerce immunities, so that providers would be liable when transmitting or hosting data uploaded by third parties in violation of data protection law. On the contrary, this provision can be understood as only meaning that the obligations concerning data protection remain only those established by the Data Protection Directive, a statement that is fully compatible with the immunity of intermediaries for third parties' violations of such obligations.*") See also M. Peguera, "The Shaky Ground of the Right to Be Delisted", *l.c.*, p. 31 et seq. ("*[…] a reading of Art. 1(5)(b) more consistent with the rest of the Directive might conclude that it does not intend to limit the scope of the safe harbors.*").

[2533] See e.g. M. V. de Azevedo Cunha, L. Marin and G. Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *l.c.*, p. 57 (arguing in favor of a uniform approach)

[2534] Article 3(3) of the Commission proposal provided that "*This Regulation should be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.*"

[2535] W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 24 ("*"it makes sense for pure infrastructure cloud providers to be treated as neutral intermediaries, unless and until they have the requisite knowledge and control over that data (in the form of access to it, at least for more than incidental purposes*").

[2536] *Ibid*, p. 27 ("*there seems no good reason why cloud providers who are neutral intermediaries, akin to hosting or caching providers under the ECD, should not benefit from similar liability defences, while also benefitting from a prohibition on having a general duty to monitor actively any data transmitted or stored by them*").

[2537] G. Sartor, "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *l.c.*, p. 570. A similar line of reasoning had also led the AG to conclude that search engines should not be considered as controllers in relation to the personal data on source web pages hosted on third-party servers.

[2538] G. Sartor, "Providers' liabilities in the new EU Data Protection Regulation", *l.c.*, p. 5 (arguing against "data protection exceptionalism") and M. V. de Azevedo Cunha, L. Marin and G. Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *l.c.*, p. 57 (arguing in favor of a uniform approach)

1248. COUNTERARGUMENTS – A first argument against incorporating the liability exemptions contained in the E-Commerce Directive is that a reasonable interpretation of the obligations of controllers and processors, which takes into account the principle of proportionality, would not result in the imposition of excessive liability. The decision of the Court of Justice in *Google Spain*, as well as the decision of the Italian Supreme Court in *Google Video*, clearly support this proposition.[2539] A second argument is that the incorporation of the liability exemptions may result in reduced protection for data subjects, particularly if the standard of care applied to intermediaries is lower than the standard that would otherwise be applied to controllers.[2540] Third, the interpretation of the concepts employed by the E-Commerce Directive (i.e., "hosting, "mere conduit" and "caching") have also given rise to a fair degree of legal uncertainty.[2541]

5.3 ASSESSMENT

1249. INTERNAL COMPARISON – The two historical solutions described above are complementary. Both represent attempts to limit the adverse effects which may arise when applying the controller and processor concepts to contexts unanticipated by the EU legislature.

1250. EXPANDING PERSONAL USE – The Court of Justice has consistently held that Directive 95/46 does not, by itself, unduly restrict legitimate uses of technology. While both the Directive and GDPR still support a certain degree of flexibility, it is clear that the existing notion of "purely personal or household activities" is overly narrow. Absent further derogations, there is a risk that data protection law will unduly interfere with individual freedom.

1251. FINAL TEXT GDPR – Despite the many arguments and constructive proposals in favor of expanding the personal use exemption, the current scope of the exemption was retained in the final version of the GDPR. Interestingly, recital (18) of the GDPR stipulates that "social networking" and "online activity" undertaken in the context of a personal or household activity falls within the remit of the personal use exemption, thus

---

[2539] Cf. *supra*; nr. 817 (*Google Video*) and nr. 1067 (*Google Spain*).

[2540] Keller, for example, argues that the standard of care incumbent upon "controllers" is more onerous (and therefore more likely to give rise to liability) than the standard of care incumbent upon internet intermediaries. See D. Keller, "Intermediary Liability and User Content under Europe's New Data Protection Law", *l.c.*, FAQ 2.

[2541] See e.g. P. Van Eecke, "Online service providers and liability: a plea for a balanced approach", *Common Market Law Review* 2011, Vol. 48, p. 1481 et seq.; E. Montéro, "Les responsabilités liées au web 2.0", *Revue du Droit des Technologies de l'Information* 2008, n° 32, p. 364 et seq. and B. Van der Sloot, "Welcome to the Jungle : the Liaiblity of Internet Intermediaries for Privacy Violations in Europe", *JIPITEC* 2015, Vol. 6, p. 214-216, available at http://www.jipitec.eu/issues/jipitec-6-3-2015/4318/van%20der%20sloot%20%283%29.pdf (last accessed 18 May 2016).

suggesting that the scope of the personal use exemption might have been implicitly widened after all.[2542]

1252. LIABILITY EXEMPTIONS – The question of whether or not to incorporate the liability exemption of the E-Commerce directive concerns, once again, the optimal specificity of legal rules.[2543] It would be possible to limit liability exposure by adopting a standard-based approach, along the lines described in the previous section.[2544] On the other hand, incorporating the rule-like liability exemptions contained in the E-Commerce Directive might yield additional benefits. First, it would further the development of a more horizontal and uniform approach to the issue of platform responsibility.[2545] In addition, article 15 of the E-Commerce Directive clearly provides that Member States may not impose general monitoring obligations upon internet intermediaries. While most would agree that internet intermediaries should not be expected to proactively monitor whether the personal data disseminated through their platform is being processed lawfully, the formal applicability of article 15 of Directive 2000/31/EC would offer certain providers greater legal certainty.

1253. CAVEATS – Applying the liability exemptions of Directive 2000/31/EC to actors involved in the processing of personal data is not a panacea: the concepts of "hosting, "mere conduit" and "caching" are subjects of continuous debate and have themselves given rise to a fair degree of legal uncertainty.[2546] Moreover, the liability exemptions of Directive 2000/31/EC would only affect the liability exposure of controllers in relation to mere distribution or storage activities. An absence of liability for mere distribution or storage does not, however, imply an absence of responsibility with regard to other operations performed on that content. Many service providers perform additional operations which go beyond a purely "intermediary", "passive", or "neutral" capacity.[2547] As a result, it may still be necessary to interpret the obligations of internet

---

[2542] See also Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Draft Statement of the Council's reasons, 5419/16 ADD 1, 17 March 2016, p. 6, accessible at http://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1/en/pdf (noting that final version of the personal use exemption was motivated by the desire to "*avoid setting rules that would create unnecessary burden for individuals*").

[2543] See also *supra*; nrs. 1203 et seq.

[2544] In particular by determining liability exposure in light of the "powers, responsibilities and capabilities" or in light of "context, role and ability to act". Cf. *supra*; nr. 1230.

[2545] M. V. de Azevedo Cunha, L. Marin and G. Sartor, "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2012, Vol. 2, No. 2, p. 57-58. This may also help to more consistently address concerns regarding the negative implications of so-called "notice and take down" mechanisms with regards to freedom of expression.

[2546] Cf. *supra*; at footnote 2541.

[2547] B. Van Alsenoy, J. Ballet, A. Kuczerawy and J. Dumortier, "Social networks and web 2.0: are users also bound by data protection regulations?", *l.c.*, p. 62.

intermediaries as controllers in light of their "responsibilities, powers and capabilities".[2548]

1254. FINAL TEXT GDPR – The proposal to incorporate the liability exemptions contained in the E-Commerce directive was retained in the final text of the GDPR. While this approach may provide greater legal certainty to certain actors, it is equally clear that many service providers will still need to assess their liability exposure in light of the liability provisions of the GDPR itself, as well as the interpretative guidance provided by the Court of Justice.

1255. INTERDEPENDENCIES – The historical solutions presented here leave the grammatical issues entirely unaffected. The incorporation of the liability exemptions of the E-Commerce Directive does, however, alleviate certain teleological issues (legal certainty) as well as certain systemic issues (scope of obligations).

[2548] Compare *supra*; nrs. 1230 et seq. See also K. Hon, E. Kosta, C. Millard and D. Stefanatou, "White paper on the proposed data protection regulation", Cloud Accountability Project, 28 February 2014, p. 21, available at http://www.a4cloud.eu/sites/default/files/D25.1%20White%20paper%20on%20new%20Data%20Protection%20Framework.pdf (last accessed 8 April 2016).

Chapter 4 RECOMMENDATIONS

1256. OUTLINE – The aim of this Chapter is to present a number of recommendations based on the analysis carried out in the previous Chapters. In contrast to the previous Chapters, however, the analysis here shall focus on the text of the GDPR, rather than on the proposals made to modify the text of Directive 95/46. The following recommendations shall be presented:

(1) abolish the concepts of controller and processor or revise the definitions;

(2) use standards and exemptions to mitigate risks of overinclusion;

(3) require the providers of processing services to implement data protection by design;

(4) enhance contractual flexibility in the relationship between controllers and processors; and

(5) expand the scope of the personal use exemption.

1 ABOLISH THE CONCEPTS OR REVISE THE DEFINITIONS

1257. SUPPORTING DIFFERENTIATION – As explained earlier, many issues associated the controller-processor model relate to the *concepts* of controller and processor, rather than the policy choice of *differentiating* between parties involved in the processing.[2549] For this reason alone, it is worth considering whether it is possible to omit the problematic concepts of controller and processor, while still supporting differentiation as regards the allocation of responsibility and risk. Using the liability provisions of the GDPR as the point of departure, the following paragraphs will outline how the GDPR might be revised to support such differentiation whilst omitting the concepts of controller and processor. Next, a proposal for possible revisions to the controller and processor and concepts will be presented.

1.1 ABOLISHING THE CONCEPTS

1258. CURRENT ARTICLE 77 GDPR – Article 77 of the GDPR currently provides that

> *"1. Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

[2549] Cf. *supra*; nr. 1211.

2. Any controller involved in the processing shall be liable for the damage caused by the processing which is not in compliance with this Regulation. A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempted from liability in accordance with paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage."[2550]

1259. REVISED ARTICLE 77 GDPR – It is perfectly possible to omit the concepts of controller and processor from article 77 GDPR while still retaining the same liability model. Under such an approach, a revised article 77 might read as follows:

1. Any person who has suffered material or immaterial damage as a result of an infringement of the Regulation shall have the right to receive compensation [...].

2. Every party involved in the processing shall be liable for the damaged caused by his own processing activities as well as processing undertaken by others on its behalf, taking into account the following limitations:

(a) a party who exclusively processes the data in accordance with the instructions of another party and on his behalf shall only be liable insofar as the damages are a result of a failure to comply with articles [list of provisions otherwise relevant to processors].

(b) any party involved in the processing may be exempted from liability insofar as he can prove that the damages are the result of an event which cannot in any way be attributed to him.

The main advantage of this approach is that it does not require parties to consider the formal legal status of each actor, but the outcome is essentially the same. Moreover, it resolves the grammatical issue which occurs by virtue of the fact that the criteria contained in the controller and processor concepts are not by nature mutually exclusive.[2551] The two substantive criteria determining the scope of a party's liability exposure are "*on behalf of*" and "*in accordance with instructions*". The proposal to use the words "on behalf of" as the main criterion to determine the scope of a party's liability

[2550] Article 77 goes on to provide that where more than one controller or processor or a controller and a processor are involved in the same processing and, where they are, in accordance with paragraphs 2 and 3, responsible for any damage caused by the processing, each controller or processor shall be held liable for the entire damage, in order to ensure effective compensation of the data subject (article 77(4)). In addition article 77(5) provides that where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage in accordance with the conditions set out in paragraph 2. While these provisions essentially codify general principles of tort law, they could be incorporated mutatis mutandis under the proposed alternative approach. For purposes of conceptual clarity, only the first 3 paragraphs of article 77 are presented here.

[2551] Cf. *supra*; nr. 1112.

exposure is based on the proposal put forward by Léonard and Mention (i.e., the "benefit-based approach"). [2552] The words "*exclusively*" and "*in accordance with the instructions of another party*" were added to clarify that a party shall only be subject to fewer data protection obligations insofar as the processing of the data in question is undertaken purely on an agency basis.[2553] To strenghten the latter point, the wording "at his request" might additionally be inserted.

1.2 REVISING THE DEFINITIONS

1260. ALTERNATIVE CRITERIA – An alternative approach would be to retain the controller and processor concepts whilst modifying their respective definitions. Using the same criteria as outlined in the previous paragraph, a controller would be defined as "*a natural or legal person, public authority, agency or any other body who processes personal data for himself or causes personal data to be processed by others on his behalf*"[2554] and the processor would be defined as "*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a controller, at its request and in accordance with its instructions*". The benefits of revising the concepts of controller and processor in this way are essentially the same as the ones outlined in the previous subsection, with the additional advantage that it requires fewer drafting changes to other provisions of the GDPR.

2 USE OF STANDARDS AND EXEMPTIONS

1261. TAILORING OBLIGATIONS – The revised liability model outlined in the previous section coincides with the liability model for controllers and processors under the GDPR. This model could easily be supplemented by a standard to support the tailoring of obligations, e.g., by adding the following provision:

> *(c) any party who has contributed to the damages suffered may be exempted from liability insofar as it demonstrates that it has implemented every reasonable measure to prevent and remove damages, taking into account its responsibilities, powers and capabilities.*"

[2552] Cf. *supra*; nr. 1166.

[2553] If the party concerned processes (or has processed) the data in question on his own initiative, i.e. outside the instructions of another party, it would in principle be subject to full panoply of data protection requirements. By adding this clarification, it is envisaged that service providers such as data brokers or the providers of search engine services shall in principle be subject to the same obligations as would otherwise be incumbent upon controllers.

[2554] The formulation "his own processing activities as well as processing undertaken by others on his behalf" was inspired by paragraph 2(3) of the German *Bundesdatenschutzgesetz* of 27 January 1977 which defined the "speicherende Stelle" as "*anyone who stores data on its own account [for its purposes] or has data stored by others*". Similar formulations were used in the French Law on Informatics, Files and Liberties (LIFL) (cf. *supra*; nrs. 327 et seq.); in the context of the preparations of the UK Data Protection Act (cf. *supra*; nr. 420) as well as in an early draft of Directive 95/46 (cf. *supra*; nr. 494).

As indicated earlier, there are benefits and costs associated with the introduction of an additional standard which supports tailoring obligations.[2555] In the end, however, the addition of this standard would merely constitute a further codification of the reasoning of the Court of Justice in *Google Spain*.[2556] As a result, one could argue that the addition of this standard would not provide added value as such. Nevertheless, it may still be beneficial to introduce the standard into the statutory text, if only to validate the approach taken by the Court of Justice and to explicitly recognise it as a valid limitation of the liability exposure to which parties involved in the processing might otherwise be subject.

1262. LIABILITY EXEMPTIONS – The revised liability model outlined above could additionally be supplemented with a reference to the liability exemptions contained in the E-Commerce Directive by simply adding a provision which reads:

> *"(d) The liability exemptions contained in E-Commerce Directive shall apply to damages suffered as a result of an infringement of the Regulation."*

Given the increase in the number of obligations directly applicable to the providers of processing services, it is appropriate to incorporate the liability exemptions contained in the E-Commerce Directive.[2557] As the EU legislature has already decided to incorporate a reference to the liability exemptions of the E-Commerce Directive in the GPDR, the proposal here is mainly aesthetic (i.e., to incorporate a reference to liability exemptions in the article concerning liability as opposed to the scope section).

3 REQUIRE DATA PROTECTION BY DESIGN FROM "PROCESSORS"

1263. DATA PROTECTION BY DESIGN – Under the GDPR, processors are not subject to the obligation to implement data protection by design. This is regrettable, given the substantial influence processors exercise in determining the means of the processing.[2558] In my view, it would be reasonable to impose a similar obligation upon

---

[2555] Cf. *supra*; nr. 1202.

[2556] Cf. *supra*; nr. 1067.

[2557] While the exemptions contained in the E-Commerce Directive will fail to address all processing activities which might merit an exemption, it will nevertheless be useful in many cases. Moreover, codification of the standard proffered by Google Spain could help to remedy the gaps which are likely to arise.

[2558] See also P. Tsormpatzoudi and F. Coudert, "Technology providers' responsibility in protecting privacy… dropped from the sky?", *Paper presented at the Amsterdam Privacy Conference* (APC), 23-26 October 2015, available at https://lirias.kuleuven.be/bitstream/123456789/508461/1/APC+Tsormpatzoudi_Coudert.pdf (noting that "*Privacy and data protection challenges stemming from the development of ICT are often related to the fact that certain data processing-related decisions are already made during the development phase. This limits the ability of the data controller to comply with the data protection framework which is only applicable from the moment that personal data are collected and processed, thus at the very end of the supply chain.*")

the providers of processing services, as long as one takes into account the intended purpose (finality) of the services they offer.[2559]

1264. ARTICLE 23(1) GDPR – Article 23(1) of the GDPR currently provides that

> "*Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*"

Extending the obligation to implement data protection by design to the providers of processing services could be realised either simply by inserting the words "*and processor*" behind the word controller, or by revising the text to reflect a passive form ("*appropriate technical and organisational measures shall be implemented*"). Under this approach, the provider of a processing service ("processor") would be responsible for designing its services and features in such a way that they facilitate compliance with data protection requirements, whereas it would be up to the customer of the processing service ("controller") to configure the services and features in the appropriate

[2559] See also Microsoft, "Protecting Data and Privacy in the Cloud", *Reactive Security Communications*, 2014, p. 3-5 (arguing that it is responsibility of cloud providers to design services in such a way that enables compliance) As early as 1972, the Younger Committee already considered that the design of a service to meet a customer's needs was an area of joint involvement and responsibility among the provider and customer of the service. See Home Office (Great Brittain), *Report of the Committee on Privacy*, *o.c.*, p. 182 et seq. Cf. supra; nr. 418. After the Younger Committee, the Lindop Committee likewise considered that it should be a requirement for computer bureaux to avoid taking on applications if it was unable to provide the relevant safeguards identified in the relevant Codes of Practice. The Committee even foresaw an advisory role for bureaux, especially towards small users who may not be aware of the contents of the relevant Codes of Practice. Cf. *supra*; nr. 425. Under the 1984 UK data protection act, not all computer bureaux needed to know what was contained in the register entry of the data user to whom it was providing services. A computer bureau which only performed the limited service of "causing data to be processed automatically" would not do anything which constituted an offence under section 5(3). If the computer bureaux provided a wider service, however, which involved collecting information on behalf of the data user or disclosing it in accordance with its instructions, it would run the risk of committing an offence if departed from the particulars contained in the user's register entry. See The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", *l.c.*, p. 6 (Question 9). Cf. *supra*; nr. 445. Today, an equivalent approach would be to impose upon the providers of value-added services a duty to of care to ensure that the legitimacy of processing has been ensured (e.g., by requiring a web analytics company to check the privacy notice of its customers to make sure that third-party analytics are covered).

manner.[2560] Providers of processing services may also be required by regulators to demonstrate compliance with the principle of privacy by design.[2561]

4 ENHANCE CONTRACTUAL FLEXIBILITY

1265. LEGAL BINDING – The GDPR has significantly increased the number of provision to be included in the contract or other legal act binding the processor to the controller. Specifically, article 26(2) GDPR provides that

> "*[t]he carrying out of processing by a processor shall be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall:*
>
> *(a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;*
>
> *(b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;*
>
> *(c) take all measures required pursuant to Article 30;*
>
> *(d) respect the conditions referred to in paragraphs 1a and 2a for enlisting another processor;*
>
> *(e) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;*
>
> *(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34 taking into account the nature of processing and the information available to the processor;*

[2560] See also Microsoft, "Protecting Data and Privacy in the Cloud", *Reactive Security Communications*, 2014, p. 10, available at http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf (last accessed 5 January 2015).
[2561] *Id.*

(g) at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data; make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions."

Article 26(2) GDPR clearly echoes the guidance of the Article 29 Working Party in relation to cloud computing.[2562] For many outsourcing scenarios, the inclusion of each of these elements in the contract or other legal act binding the processor to the controller may well be appropriate. As indicated earlier, however, there may be situations in which the inclusion of each of these elements in every type of outsourcing arrangement may be excessive. For example, the provider of an IaaS service, who hosts encrypted data on behalf of a SaaS or PaaS provider, may not need to know which types of personal data are being stored on its servers.[2563] Its ability to assist the controller in accommodating data subject rights may, for the same reason, be non-existent. In other words, the rules contained in article 26(2) may be overinclusive[2564].

1266. ALTERNATIVE – The duty to ensure appropriate legal binding of parties processing personal data on behalf of others should be replaced by a more flexible standard (e.g., "*any party who enlists another party to process personal data on his behalf shall adduce adequate safeguards*").[2565] The inclusion of such a standard, as an alternative to the rule contained in, would closely resemble the approach of the Canadian Privacy Act (PIPEDA).[2566] Schedule 5 of PIPEDA sets forth the basic data principles with which a "responsible organisation" must comply. The first of these principles is the principle of accountability. Clause 4.1 identifies a variety of measures that responsible organisations must implement in order to comply with this

---

[2562] Cf. *supra*; nr. 947.

[2563] See also K. Hon, E. Kosta, C. Millard and D. Stefanatou, "White paper on the proposed data protection regulation", *l.c.*, p. 19 ("*The Council would require the controller-processor contract to cover 'the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects'. This echoes WP196 but does not suit self-service infrastructure cloud services, where the provider would not know the subject matter, nature or purpose of processing, etc, unless it inspected data or monitored processing, which the controller would positively not wish the provider to do; nor would the controller wish to give such information to the provider, let alone be required to do so in the contract.*")

[2564] It should be noted, however, that article 26(2)e and 26(2)f both contain standards to mitigate risks of overinclusiveness (e.g., "*taking into account the nature of the processing*", "*insofar as this is possible*", and "*taking into account the information available to processors*")

[2565] Cf. *supra*; nr. 1233.

[2566] Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, available at http://laws.justice.gc.ca/PDF/Statute/P/P-8.6.pdf (last accessed 30 November 2010). See also W. Kuan Hon, C. Millard and I. Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *l.c.*, p. 28.

principle.[2567] The accountability principle requires, inter alia, that responsible organisations take all reasonable steps to protect personal information under their control, regardless of where it is processed.[2568] In particular, organisations are considered to remain responsible for the actions by third parties to whom data has been "transferred".[2569] In other words, while PIPEDA does not make a formal distinction between controllers and processors, it does contain provisions aimed at achieving a similar effect, namely ensuring that personal information is guaranteed a comparable level of protection while the information is being processed by a third party.[2570] This approach has a number of advantages. The first is that it enables greater flexibility, while at the same time reinforcing the notion that the responsible organisation is obligated to adduce adequate safeguards when engaging other actors to help achieve its objectives. A second advantage is that it does not rely upon the formal qualification of the actor to whom the information has been transferred; thus having the potential to mitigate some of the adverse impacts resulting from the underinclusive nature of the controller-processor model.[2571]

1267. ROLE OF REGULATORY GUIDANCE – Replacing the rule of article 26(2) with a standard would imply sacrificing certain benefits, in particular as regards specificity and

---

[2567] The principle of accountability received considerable attention in the context of the review of Directive 95/46. See e.g. Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability", WP 173, 13 July 2010, 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, last accessed 8 February 2011; European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "A comprehensive approach on personal data protection in the European Union", November 2010, Brussels, COM(2010) 609 final, 12, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf, last accessed 8 February 2011). Readers familiar with these discussions shall be aware that accountability is a relatively "amorphous" concept, which can mean different things to different people (see also A. Sinclair, "The Chameleon of Accountability: Forms and Discourses", *Accounting, Organisations and Society* 1995, vol. 20, no 2/3, p. 219; M. Bovens, "Analysing and Assessing Accountability: A conceptual Framework", *European Law Journal* 2007, vol. 13, no. 4, p. 448). For more information on the different meanings associated with accountability, as well as the role that the accountability principle has played in various instruments of data protection over time see J. Alhadeff, B. Van Alsenoy and J. Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.,* p. 50 et seq.

[2568] Office of the Privacy Commissioner of Canada, "PIPEDA - Processing Personal Data Across Borders Guidelines", 2009, 8, available at http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf (last accessed 1 December 2010).

[2569] J. Alhadeff, B. Van Alsenoy and J.Dumortier, "The accountability principle in data protection regulation: origin, development and future directions", *l.c.*, p. 55. Note that the term "transfer" has a very specific meaning in PIPEDA, which is to be contrasted with "disclosure". See Office of the Privacy Commissioner of Canada, "PIPEDA - Processing Personal Data Across Borders Guidelines", *l.c.*, 5. A "transfer" is understood as an exchange of information whereby its use is confined to the purpose for which it was collected (Ibid, 5). A "disclosure", on the other hand, concerns an exchange of information for a purpose which was previously not yet identified. This distinction bears considerable resemblance to some of the guidance provided by the Working Party in Opinion 1/2010, where it is indicated that when a processor either re-uses data it for a different purpose or otherwise acts beyond the instructions given by a controller, its qualification as a processor will change to that of controller for these processing operations (see Opinion 1/2010, *l.c.*, in particular p. 14).

[2570] See also clause 4.1.3 of Section 5 of PIPEDA.

[2571] Cf. *supra*; nr. 1208.

legal certainty. I would submit, however, that additional specificity and legal certainty could be provided through regulatory guidance, as was already being done under Directive 95/46.

5 EXPAND THE SCOPE OF THE PERSONAL USE EXEMPTION

1268. ARTICLE 2(2)b GDPR – Article 2(2)b of the GDPR specifies that the Regulation shall not apply to the processing of personal data "*by a natural person in the course of a purely personal or household activity*". This wording is identical to the wording of article 3(2) of Directive 95/46/EC. Interestingly, recital (18) of the GDPR stipulates that "social networking" and "online activity" undertaken in the context of a personal or household activity fall within the remit of the personal use exemption, thus suggesting that the scope of the personal use exemption might have been widened ever-so-slightly after all.[2572]

1269. DEROGATIONS POSSIBLE – The conceptual approach outlined by the Court of Justice in *Ryneš* suggested that Directive 95/46 can (and should) be implemented in such a way that it does not unduly restrict individuals' ability to pursue a legitimate objective. Under the GDPR, Member States have retained similar abilities to restrict the application of certain provisions by means of national legislation. It is up to the Member States, however, to actually provide for appropriate derogations. A significant number of Member States have already introduced specific rules governing the use of CCTV, including by private individuals.[2573] Beyond CCTV, however, it seems only few States have introduced specific derogations.[2574] Without ruling out the possibility such

[2572] See also the Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Draft Statement of the Council's reasons, 5419/16 ADD 1, 17 March 2016, p. 6 (noting that the final version of the personal use exemption was motivated by the desire to "avoid setting rules that would create unnecessary burden for individuals"). See also, however, the (modified) position of the Article 29 Working Party, as expressed prior to the trilogue negotiations: Article 29 Data Protection Working Party, "Letter from the Art. 29 WP to MEP Jan Philipp Albrecht in view of the trilogue - Appendix Core topics in the view of trilogue", 17 June 2015, p. 3, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf (last accessed 8 April 2016) ("*The Working Party recognizes the Council of the EU's aim to slightly broaden the scope of the household exemption in order to limit the scope of the Regulation but feels that any exceptions to the rules shall be formulated and interpreted restrictively. […] The Working Party is in favour of a limited and carefully balanced household exemption applying to "purely" household activities as provided for in Directive 95/46/EC and interpreted by ECJ case law.*") The ultimate return to the original wording of article 3(2) of Directive 95/46 suggests a desire not to call into question previous case law of the Court of Justice regarding the scope of the personal use exemption.

[2573] See D. Korff, *EC Study on Implementation of Data Protection Directive 95/46/EC*, Study Contract ETD/2001/B5-3001/A/49, 2002, 135 et seq., accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 (last accessed 8 April 2016).

[2574] Idem.

derogations may still be introduced, it is likely they will lag behind technical and societal developments. Moreover, as this measure is not harmonized at Community level, the risk of fragmentation is considerable.[2575]

1270. EXPANDING PERSONAL USE – In my opinion, the personal use exemption should apply to all activities which may reasonably be construed as taking place in the course of an individual's private or family life. In addition, an individual should be able to benefit from the personal use exemption regardless of the recipients involved.[2576] Instead, the terms "private and family life" should (continue to) be interpreted broadly, extending to any activities related to the development of one's personal identity or the establishment of relationships with others.[2577] Only when the risk of excessive interference in the privacy interests of others is evident (e.g., due to the scale or frequency of the processing, combined with the recipients and nature of the data), might it be proportionate to bring the activities of private individuals within the scope of data protection law. In order to promote legal certainty, additional criteria establishing the boundaries of the personal use exemption should be anchored in the law.

1271. ALTERNATIVE – Article 2(2)b of the GDPR should be revised to specify that the Regulation shall not apply to the processing of personal data "*by a natural person in the context of his or her private or family life*". Omitting the word "purely" encourages a broader understanding of the personal use exemption, thereby considerably mitigating risks of overregulation. In addition, by explicitly referring to the terms "private and family life", as the Court of Justice did in *Lindqvist*[2578], it would be made clear that that any activities related to the development of one's personal identity or the establishment of relationships with others should in principle fall within the remit of the personal use exemption. The revision of article 2(2)b GDPR might additionally be complemented by

---

[2575] Of course, one might argue that the use of a general standard to delineate the scope of the personal use exemption, as opposed to introducing a rule, will also give rise to an absence of legal certainty. While it is recognized that there will still be some legal uncertainty and national differences due to potential for different weighting of different criteria, it can also be argued that with further guidance from Court of Justice, WP29 and EDPS eventually a consistent application will emerge. See also N. Xanthoulis, "Negotiating the EU Data Protection Reform: Reflections on the Household Exemption", *l.c.*, p. 148-149. ("*The vast variety of users' online activities, particularly the ones that involve UGC and participation in SNS, prevent the EU legislator from sufficiently providing for a clear-cut definition of private conduct (as opposed to activity done in public), thus, leading us to conclude that a fair, efficient and practical solution would only be achieved if the matter is left to be subsequently determined on case by case basis, by national courts and competent authorities and eventually the CJEU. Such long process might result to the initial fragmentation of the interpretation of proposed Regulation's scope, at least in the short term, before a homogenous application of the proposed exemption is achieved.*")

[2576] This would effectively require reversing the second part of personal use test advanced by *Lindqvist*.

[2577] The European Court of Human Rights has underlined that it also protects a right to identity and personal development, and the right to establish and develop relationships with others. (European Court of Human Rights, *P.G. and J.H. v. United Kingdom*, 25 September 2001, application no. 44787/98, paragraph 56 and European Court of Human Rights, *Niemietz v. Germany*, 16 December 1992, application no. 13710/88, paragraph 29; available at http://www.echr.coe.int).

[2578] The first part of the "personal use" test promulgated by the ECJ in *Lindqvist* also refers to "in the course of private or family life of individuals" (Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596, paragraph 74).

the criteria proposed by the Article 29 Working Party in its 2013 Statement.[2579] After all, the criteria proposed by the Article 29 Working Party would offer useful guidance when determining whether an activity might no longer be considered as taking place "*in the context of his or her private of family life*". In other words: the Working Party criteria would help to promote legal certainty, while still preserving a much needed degree of flexibility.

[2579] Cf. *supra*; nr. 1242.

Chapter 5 CONCLUSION

1272. MAIN RESEARCH QUESTION – The distinction between controllers and processors is central to European data protection law. Unfortunately, certain technological and social developments have rendered it increasingly difficult to apply this model in practice, thereby leading to legal uncertainty. The main research question this thesis set out to answer is whether the allocation of responsibility and risk among actors involved in the processing of personal data, as set forth by Directive 95/46 and the General Data Protection Regulation, could be revised in a manner which increases legal certainty while maintaining at least an equivalent level of data protection.[2580] In order to answer this question, four sub-questions helped guide the research, namely[2581]:

1. What is the nature and role of the controller and processor concepts under European data protection law?
2. What is the origin of the controller-processor model and how has it evolved over time?
3. What are the types of issues that arise when applying the controller-processor model in practice?
4. Which solutions have been proposed to address the issues that arise in practice and to what extent are they capable of addressing the issues?

1273. NATURE AND ROLE OF CONCEPTS – The concept of a controller is a *functional* concept: it enumerates a set of criteria with a view of allocating responsibilities upon those actors who exercise significant factual influence over the processing. The processor concept likewise serves to allocate responsibility, but is dependent primarily on a decision of a controller to enlist a separate actor to process personal data on its behalf. The primary role of both the controller and processor concepts is to allocate responsibility. In addition, both the controller and processor concepts play an important role in the determination of which law(s) applies (apply) to the processing, and in the determination of what is required in order to comply with certain substantive provisions of European data protection law.

1274. ORIGIN AND DEVELOPMENT – Before the term "controller" became a term of art, those responsible for ensuring compliance with data protection laws went by many names. Despite notable differences in terminology, two recurring elements can be distinguished. The first element is the element of *mastery*: the actor designated as being responsible for compliance had the ability to exercise power over the processing, in one form or another. A second recurring element involves the concept of *gain*: responsibility

[2580] Cf. *supra*; nr. 17.
[2581] Cf. *supra*; nr. 22.

was bestowed upon the entity which reaps the benefits of the output of the processing. From the very first data protection laws, policymakers were also mindful of the fact that data processing frequently involved outsourcing. Nevertheless, the concept of a "processor", understood as a third party who processes data as a service to others, was mainly present in the background. It was not until the late 1970's that the providers of processing services received formal recognition, worthy of their own statutory definitions. Central to each of these definitions was the notion of *agency*: the "processor" was always understood as an entity acting on behalf of someone else, without personal interest in the output of the processing activity. Once created, the controller-processor model served mainly to ensure a continuous level of protection for data subjects in cases of outsourcing. While the controller was generally deemed "ultimately" responsible for compliance, several national laws also imposed obligations directly upon processors. At EU level, a similar pattern emerged: while processors were mainly indirectly accountable under Directive 95/46, the General Data Protection Regulation imposes a host of requirements directly upon processors and renders them accountable towards regulatory authorities and data subjects.

1275. TYPOLOGY OF ISSUES – Experts frequently disagree as to whether an actor should be considered a "controller" or "processor", or struggle to make an unambiguous determination. Four categories of issues can be distinguished: (1) issues that concern the words chosen to define the concepts of controller and processor (*grammatical issues*); (2) issues that concern the policy objectives that underlie the allocation of responsibility and risk between controllers and processors (*teleological issues*); (3) issues that arise in light of the functions fulfilled by the controller and processor concepts (*systemic issues*); and (4) issues that arise when applying the controller-processor model to situations which were not envisaged by the European legislature (*historical issues*). The teleological issues are perhaps the most troubling, as they imply that the policy objectives underlying the distinction between controllers and processors may be difficult to realise in practice. The grammatical, systemic and historical issues have merely amplified the call for legislative change over time.

1276. PROPOSED SOLUTIONS – The review of Directive 95/46 triggered a variety of proposals to remedy the shortcomings of the existing framework. While changing the definitions themselves might have been beneficial, none of the proposed solutions appeared satisfactory. Other proposals went to the heart of the controller-processor model, advocating either its abolition or partial assimilation of the functions fulfilled by both concepts. In addition, a number of modifications were proposed to address the need for increased flexibility when applying the existing framework to current processing realities.

1277. APPROACH OF THE GDPR – With the new General Data Protection Regulation, European legislature made a number of significant changes to the controller-processor model. While it retained the basic concepts of controller and processor, it considerably

reduced the systemic importance of the distinction between the two, in particular by providing greater recognition to situations of joint control and by imposing a number of obligations directly upon processors. The incorporation of the liability exemptions of the E-Commerce Directive additionally helps to mitigate risks of unintended consequences when applying data protection law in cases where personal data are processed through the Internet.

1278. RECOMMENDATIONS – The changes introduced by the GDPR are likely to be sufficient for the time being. In the longer, however, it may become necessary to introduce further changes. In this regard, a number of recommendations can be made. First, the possibility of abolishing the distinction between controllers and processors should receive further consideration. It is possible to implement the same policy choices without retaining these problematic concepts. Alternatively, the definitions of each concept could be revised to include less ambiguous and mutually exclusive criteria. Second, the legislature should consider the use of standards (as opposed to rules) to mitigate certain risks of overinclusion. Third, I believe the obligation to implement data protection by design should eventually also be made directly applicable to the providers of processing services, given their important role in determining the means of the processing. Fourth, the legal framework should allow for contractual flexibility in the relationship between "controllers" and "processors", leaving room for greater specificity in the form of regulatory guidance. Finally, the scope of the personal use exemption should be expanded. Other legal constructs, such as tort law and personality rights, are better suited to regulate conflicts between private individuals. It is up to all of us to develop these constructs further, and to inform them with data protection considerations as needed.

BIBLIOGRAPHY

1 LEGISLATION AND IMPLEMENTING ACTS

COUNCIL OF EUROPE

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.

EUROPEAN UNION

Convention implementing Schengen agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 19 June 1990, *O.J.* 22 September 2000, L 239/19.

Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, *O.J.* 23 November 1995, L 281/31.

Council Decision of 6 November 1995 on a Community contribution for telematic interchange of data between administrations in the Community (IDA) (95/468/EC), *O.J.* 11 November 1995, L 269/23.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures, *O.J.* 19 January 2000, L 13/12.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *O.J.* 17 July 2000, L 178/1.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *O.J.* 12 January 2001, L 8/1.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O.J.* 31 July 2002, L 201/37.

Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), *O.J.* 18 May 2004, L-181/25 (corrig.).

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, *O.J.* 17 December 2007, C 306.

European Commission, Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data, *O.J.* 16 January 2008, L 13/18.

Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *O.J.* 30 December 2008, L 350/60.

European Commission, Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), 2009/329/EC, *O.J.* 18 April 2009, L 100/17.

Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA), *O.J.* 3 October 2009, L-260/20.

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), 2010/87/EU, *O.J.* 12 February 2010, L 39/5.

Regulation No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal market Information system and repealing Commission Decision 2008/49/EC, *O.J.* 14 November 2012, L 316/1.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC , *O.J.* 28 August 2014, L 257/73.

European Commission, Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, *O.J.* 9 September 2015, L 235/1.

European Commission, Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on

electronic identification and trust services for electronic transactions in the internal market, *O.J.* 9 September 2015, L 235/7.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* 4 May 2016, L 119/1.

NATIONAL LEGISLATION

Law of 16 December 1969 establishing the data processing centre of the State of Hesse and regarding the data processing centres of local communities, *HE GVBI*, 22 December 1969, Nr. 32, Part I, p. 304 (Hesse).

Data Protection Act of 7 October 1970, *HE GVBI*. 12 October 1970, nr. 41, Part I, p. 625 (Hesse).

Law of 4 September 1974, *HE GVBl.* 9 September 1974, nr. 27, I, p. 365 (Hesse).

Law of 31 January 1978, *HE GVBl.* 7 February 1978, nr. 4, I, p. 96 (Hesse).

Law of 11 November 1986, *HE GVBl.* 20 November 1986, nr. 25, I, p. 309 (Hesse).

Law of 5 November 1998, *HE GVBl.* 9 November 1998, nr. 22, I, p. 421(Hesse).

Data Act of 11 May 1973 ("*Datalagen*"), *SFS* 1973: 289 (Sweden).

Private Register Act ("*Lov om private register*") of 8 June 1978 (nr. 293) (Denmark).

Act no. 48 of 9 June 1978 relating to personal data filing systems (Norway).

Law n° 70-643 of 17 July 1970 seeking to reinforce the protection of the rights of individuals and citizens, *J.0.* 19 July 1970, p. 6755 (France).

Decree n° 74-938 of 8 November 1974 establishing the Committee on Informatics and Liberties, *J.O.* 13 November 1974, p. 11403 (France).

Federal Data Protection Act of 27 January 1977, *BGBl.* I Nr. 7 S. 201 (Germany).

Law n° 78-17 of 6 January 1978 concerning informatics, files and liberties, *J.O.*7 January 1978, p. 227 (corr. 25 January 1978) (France).

Federal Act of 18 October 1978 on the protection of personal data, *Bundesgesetzblatt für die Republik Österreich* 1978, 193. Stück, p. 3619 (Austria).

Law of 31 March 1979 regulating the use of personal data in automated data processing, *Journal Officiel du Grand-Duché de Luxembourg* 11 April 1979, N° 29, p. 581 (Luxembourg).

Law n° 94-548 of 1 July 1994 concerning the processing of personal data for purposes of medical research purposes modifying the law n° 78-17 of 6 January 1978 concerning informatics, files and liberties, *J.O.* 2 July 1994, p. 25 (France).

Law n° 2004-801 of 6 August 2004 concerning the protection of natural persons with regards to the processing of personal data and modifying Law n° 78-17 of 6 January 1978 concerning informatics, files and liberties, *J.O.* 7 August 2004, p. 24 (France).

Right to Privacy Bill, *HC Deb* 26 November 1969, vol. 792, c. 430 (United Kingdom)

Act No. 101/2000 Coll. Of 4 April 2000 on the Protection of Personal Data (Czech Republic).

Law of 8 August 1983 organising a register of natural persons, *B.S.*, 21 March 1984 (Belgium).

Law of 15 January 1990 establishing and organising a Crossroadsbank for Social Security, *B.S*. 22 February 1990 (Belgium).

Law of 17 June 1991 approving the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, drawn up in Strasbourg on 28 January 1981, *B.S.* 30 December 1993 (Belgium).

Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, *B.S.* 18 March 1993 (Belgium).

Law of 6 July 2000 containing rules regarding the protection of personal data (Data Protection Act), *Staatsblad* 302 (Netherlands),

Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, (Canada).

2 PREPARATORY WORKS

DIRECTIVE 95/46

Debates of the European Parliament, Report of Proceedings from 12 to 16 November 1973, 1973-1974 Session, *O.J.* November 1973, Annex No. 168p. 104 (reply to Oral Question 122/73).

Legal Affairs Committee, Interim Report on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing, 19 February 1975, *European Parliament Working Documents* 1974-1975, Document 487/74.

European Parliament, Resolution of the European Parliament on the protection of the rights of the individual in the face of the technical developments in data processing, *O.J.* 13 March 1975, C 60/48.

European Parliament, Resolution of the European Parliament on the protection of the rights of the individual in the face of the technical developments in data processing, *O.J.* 3 May 1976, C100/27; *O.J.* 5 June 1979, C 140/34-38 and *O.J.* 5 April 1982, C87/39-41.

Commission of the European Communities, Recommendation 81/679/EEC of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data, *O.J.* 29 August 1981, L 246/31.

Commission of the European Communities, Commission Communication on the Protection of individuals in relation to the processing of personal data in the Community and information security, COM(90) 314 final, SYN 287 and 288, 13 September 1990.

European Parliament, Committee on Economic and Monetary Affairs and Industrial Policy, Working Document on data protection (COM(90) 314 fin.), drafted by Mr. F. Herman, 26 February 1991, PE 148.204, 11 p.

Economic and Social Committee, "Opinion on: the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data; the proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks; and — the proposal for a Council Decision in the field of information security (91/C 159/14), *O.J.* 17 June 1991 C 159/38.

European Parliament, Position of the European Parliament on Proposal for a directive I COM (90) 0314 - C3-0323/90 - SYN 287 / Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data T3-0140/1992, 11 March 1992 (First Reading) *O.J.* 13 April 1992, C 94/173-201.

Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/30-61.

Commission of the European Communities, Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (92) 422 final - SYN 287, 15 October 1992, *O.J.* 27 November 1992, C 311/39.

Council of the European Union, Common position (EC) No 1/95 adopted by the Council on 20 February 1995 with a view to adopting Directive 95/.../EC of the European Parliament and of the Council of ... on the protection of individuals with regard to the

processing of personal data and on the free movement of such data, *O.J.* 13 April 1995, C 93/1-24.

Commissie juridische zaken en rechten van de burger, "Aanbeveling voor de tweede lezing betreffende het gemeenschappelijke standpunt van de Raad met het oog op de aanneming van de richtlijn van het Europese Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (C4-00051/95 – 00/0287(COD)), PE 212.057/def, A4-0120/95, 24 mei 1995.

European Parliament, Decision of the European Parliament on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (C4-0051/95 - 00/0287(COD)), *O.J.* 3 July 1995 C 166/105-107.

Commission of the European Communities, Opinion of the Commission pursuant to Article 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a European Parliament and Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (95) 375 final- COD287, 18 July 1995.

GENERAL DATA PROTECTION REGULATION

European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, COM(2010) 609 final, November 2010.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 2012/0011 (COD), 25 January 2012.

European Commission, "Evaluation of the implementation of the Data Protection Directive", Annex 2 of Commission Staff Working Paper, Impact Assessment, SEC(2012) 72 final, 25 January 2012.

Council of the European Union, Working Party on Information Exchange and Data Protection (DAPIX), "Outcome of proceedings – summary of discussions on 23-24 February 2012", 2012/0011 (COD), 7221/12, DAPIX 22, 8 March 2012.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238/2, 4 June 2012.

European Parliament, LIBE Committee, "Working Document 2 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), PE497.802v01-00, 8 October 2012.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) 16 January 2013.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)) Compromise amendments on Articles 1-29, 7 October 2013.

Committee on Civil Liberties, Justice and Home Affairs, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), 21 November 2013.

Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) – Specific Issues of Chapters I-IV of the General Data Protection Regulation – certain aspects of the relationship between controllers and processors, 2012/0011 (COD), 5345/14, 15 January 2014.

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 12 March 2014.

Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection on the proposed General Data Protection Regulation – Chapter IV, 2012/0011 (COD), 12312/14, 1 August 2014.

Council of the European Union, Note from CZ, DE, IE, ES, FR, HR, NL, AT, PL, PT, FI and UK delegations to the Working Group on Information Exchange and Data Protection (DAPIX), 2012/0011 (COD), 7586/1/15 REV 1, 10 April 2015.

Council of the European Union, Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX) on the General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 7722/15, 13 April 2015.

Council of the European Union, Note from the German delegation to the Working Group on Information Exchange and Data Protection (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/15, 21 April 2015.

Council for the European Union, Note from the Presidency to the JHA Counsellors DAPIX on a Proposal for a General Data Protection Regulation – Chapter VIII, 8371/15, 4 May 2015.

Council of the European Union, Note from the German delegation to the JHA Counsellors (DAPIX) on the Proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8150/1/15, 6 May 2015.

Council of the European Union, Note from the Presidency to the Permanent Representatives Committee on the proposal for a General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 8383/15, 13 May 2015.

Council of the European Union, Note from Presidency to JHA Counsellors on the proposed General Data Protection Regulation – Chapter VIII, 2012/0011 (COD), 9083/15, 27 May 2015.

Council for the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach", 2012/0011 (COD), 9565/15, 11 June 2015.

Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Political agreement", 5455/16, 28 January 2016.

Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Draft Statement of the Council's reasons, 5419/16 ADD 1, 17 March 2016, accessible at http://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1/en/pdf

Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection

Regulation), 5419/16, 6 April 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

European Commission, Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union concerning the position of the Council on the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, COM(2016) 214 final, 11 April 2016.

NATIONAL LEGISLATION

Assemblé Nationale, Projet de loi relatif à l'informatique et aux libertés, Enregistré à la Présidence de l'Assemblée national le 9 aout 1976, Annexe au procès-verbal de la séance du 2 octobre 1976, *Document Parl.* no. 2516, p. 1-18 (France).

HL Deb 21 December 1982, vol. 437 c. 926 (United Kingdom).

HL Deb 20 January 1983 vol. 437 cc 1551 (United Kingdom).

HL Deb 10 March 1983 vol. 440, at cc 373 (United Kingdom).

HL Deb, 24 March 1983, vol. 440, at cc 1275 (United Kingdom).

HL Deb, 5 July 1983, vol. 443, at cc 509 (United Kingdom).

HL Deb, 19 July 1983, vol. 443, cc 1068 (United Kingdom).

HL Deb, 21 July 1983, vol. 443, cc 1299 (United Kingdom).

Voorstel van wet betreffende de bescherming van het privé-leven en de persoonlijkheid, *Parl. St.* Senaat, 1970-1971, 19 juli 1971, nr. 706 (Belgium).

Wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St. Kamer*, 1990-1991, 6 May 1991, nr. 1610-1 (Belgium).

Memorie van Toelichting, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St. Kamer*, 1990-1991, 6 May 1991, nr. 1610-1 (Belgium)

Verslag namens de Minister van Justitie uitgebracht door Mevr. Merckx-Van Goey, Wetsontwerp ter bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St. Kamer*, 1991-1992 (B.Z.), 2 July 1992, nr. 413-12 (Belgium).

Verslag namens de commissie voor de Justitie uitgebracht door de heer Vandenberghe, *Gedr. St.* Senaat, 1991-1992 (B.Z.), 27 October 1992, nr. 445-2 (Belgium).

Raad van State, Advies van de Raad van State bij het voorontwerp van wet tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij Verkeer van die gegevens, 2 February 1998, *Parl. St. Kamer* 1997-1998, nr. 1566/1 (Belgium).

Tweede Kamer der Staten-Generaal, Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens) – Memorie van Toelichting, Vergaderjaar 1997-1998, 25 892, nr. 3 (Netherlands).

3 CASE LAW

EUROPEAN COURT OF HUMAN RIGHTS

European Court of Human Rights, P.G. and J.H. v. United Kingdom, 25 September 2001, application no. 44787/98.

European Court of Human Rights, Niemietz v. Germany, 16 December 1992, application no. 13710/88.

COURT OF JUSTICE OF THE EUROPEAN UNION

Judgement in *Bodil Lindqvist*, C-101/01, EU:C:2003:596.

Judgement in *Kalliopi Nikolaou*, T-259/03, EU:T:2007:254.

Judgement in *Satamedia*, Case C‑73/07, EU:C:2008:266.

Judgement in *Fotios Nanopoulos*, F-30/08, EU:F:2010:43.

Judgement in *Volker und Markus Schecke*, Joined Cases C‑92/09 and C‑93/09, EU:C:2010:662.

Judgement in *Google Spain*, C-131/12, EU:C:2014:317.

Judgement in *Smaranda Bara and Others*, C‑201/14, EU:C:2015:638.

Judgement in *František Ryneš*, C‑212/13, EU:C:2014:2428.

Judgment in *Weltimmo*, C‑230/14, EU:C:2015:639.

Opinion of Advocate-General Campos Sánchez-Bordana in *Breyer*, C‑582/14, ECLI:EU:C:2016:339.

NATIONAL CASE LAW

Bundesverfassungsgericht, Decision of 15 December 1983 regarding Volkzählungsgesetz 83, *BVerfGE* vol. 65, p. 1 (Germany).

United States Supreme Court, *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989) (United States).

Kh. Kortrijk, 1ste Kamer, 19 June 2003, *T.G.R.* 2007, p. 96 (Belgium).

Gent, 6 January 2005, *T.G.R.* 2007, p. 92 (Belgium).

Cour d'Appel de Liège, 7ième Chambre, Bobon Benjamin / SPRL Diablo, 2008/RG/1165, 19 November 2009 (Belgium).

Corte di Cassazione, sez. III Penale, sentenza 17 dicembre 2013 – deposit ail 3 febbraio 2014, sentenza n. 5107/14 (Italy).

High Court of Justice, *Applause Store Productions Limited and Matthew Firsht v. Grant Raphael*, 24 July 2008, [2008] EWHC 1781 (QB) (United Kingdom).

High Court of Justice, *Stephen Robins and Gabbitas Robins v. Rick Kordowski and Tim Smee*, 22 July 2011, [2011] EWHC 1912 (QB) (United Kingdom).

Court of Appeal (Civil Division), *Google Inc v Vidal-Hall & Ors* [2015] EWCA Civ 311 (United Kingdom).

Tribunal Supremo. Sala de lo Civil, A and B v Ediciones El Pais, Judgment number 545/2015, ECLI:ES:TS:2015:4132 (Spain).

Cour de Cassation, Arrêt C.15.0052.F, 29 April 2016 (Belgium).

4 REGULATORY OPINIONS AND GUIDANCE

ARTICLE 29 WORKING PARTY

Article 29 Data Protection Working Party, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", WP 56, 30 May 2002.

Article 29 Data Protection Working Party, "Working Document on on-line authentication services", WP 68, 29 January 2003.

Article 29 Data Protection Working Party, "Working document on E-Government", WP 73, 8 May 2003.

Article 29 Data Protection Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)", WP 128, 22 November 2006.

Article 29 Data Protection Working Party, "Working Document on the processing of personal data relating to health in electronic health records (EHR)", WP 131, 15 February 2007.

Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data", WP 136, 20 June 2007.

Article 29 Data Protection Working Party, "Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)", WP 140, 20 September 2007.

Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines", WP 148, 4 April 2008.

Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", WP 163, 12 June 2009.

Article 29, "The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", WP 168, 1 December 2009.

Article 29 Data Protection Working Party, "Opinion 1/2010 on the concepts of 'controller' and 'processor'", WP 169, 16 February 2010.

Article 29 Data Protection Working Party, "Opinion 2/2010 on online behavioural advertising", WP 171, 22 June 2010.

Article 29 Data Protection Working Party, "Opinion 3/2010 on the principle of accountability", WP 173, 13 July 2010.

Article 29 Data Protection Working Party, "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC", WP 176, 12 July 2010.

Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", WP 179, 16 December 2010.

Article 29 Data Protection Working Party, Biometrics & eGovernment Subgroup, "Written Report concerning the STORK Project", Ref.Ares(2011)424406, 15 April 2011.

Article 29 Data Protection Working Party, "Opinion 01/2012 on the data protection reform proposals", WP 191, 23 March 2012.

Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing", WP 196, 1 July 2012.

Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", WP 202, 27 February 2013.

Article 29 Data Protection Working Party, "Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities", 27 February 2013.

Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", WP 203, 2 April 2013.

Article 29 Data Protection Working Party, "Working document 01/2014 on Draft Ad hoc contractual clauses 'EU data processor to non-EU sub-processor'", WP 214, 21 March 2014.

Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12", WP 225, 26 November 2014.

Article 29 Data Protection Working Party, "Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing", WP 232, 22 September 2015.

Article 29 Data Protection Working Party, "Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, WP 179 update", 16 December 2015.

EUROPEAN DATA PROTECTION SUPERVISOR

European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data (2008/49/EC) (2008/C 270/01)", *O.J.* 25 October 2008, C 270/1.

European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('IMI')", 22 November 2011.

European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the data protection reform package", 7 March 2012.

European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)", 27 September 2012.

European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of Cloud Computing in Europe'", 16 November 2012.

European Data Protection Supervisor (EDPS), "Additional EDPS comments on the Data Protection Reform Package", 15 March 2013.

NATIONAL DATA PROTECTION AUTHORITIES

Data Protection Registrar, "The Data Protection Act 1984: An introduction to the act and guide for data users and computer bureaux", Data Protection Registrar, Wilmslow, 1985.

The Data Protection Registrar, "The Data Protection Act of 1984: Questions and Answers on the Act (1-20)", Office of The Data Protection Registrar, Wilmslow, 1985.

Data Protection Registrar, "The Data Protection Act 1984: The Definitions", Great Britain. Office of the Data Protection Registrar, Wilmslow, 1989.

Information Commissioner's Office (ICO), "Data Protection Act, 1998 - Legal Guidance", Version 1, not dated.

Information Commissioner's Office (ICO), "Outsourcing - A guide for small and medium-sized businesses", v1.0, 28 February 2012.

Information Commissioner's Office (ICO), "Guidance on the use of cloud computing", v1.1, 2 October 2012.

Information Commissioner's Office (ICO), "Proposed new EU General Data Protection Regulation: Article-by-article analysis paper", v1.0, 12 February 2013.

Information Commissioner's Office (ICO), "Social networking and online forums – when does the DPA apply?", version 1.0, 24 May 2013.

Commissie voor de Persoonlijke Levenssfeer, Advies Nr 37/2006 van 27 september 2006 betreffende de doorgifte van persoonsgegevens door de CVBA SWIFT ingevolge de dwangbevelen van de UST (OFAC).

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Aanbeveling nr. 02/2007 uit eigen beweging inzake de verspreiding van beeldmateriaal", 28 November 2007.

Commissie voor de Persoonlijke Levenssfeer, "Decision of 9 December 2008 regarding the Control and recommendation procedure initiated with respect to the company SWIFT", 9 December 2008.

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, "Aanbeveling nr 09/2012 uit eigen beweging in verband met authentieke gegevensbronnen in de overheidssector (CO-AR-2010-005)", 23 May 2012.

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Sectoraal Comité van de Sociale Zekerheid en van de Gezondheid, Afdeling «Gezondheid», Beraadslaging nr. 11/088 van 18 oktober 2011, gewijzigd op 9 juni 2015, met betrekking tot de nota betreffende de elektronische bewijsmiddelen van een therapeutische relatie en van een zorgrelatie, SCSZG/15/088.

Commission National Informatique et Libertés (CNIL), "Les transferts de données à caractère personnel hors Union européenne", not dated.

Commission National Informatique et Libertés (CNIL), "Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques", September 2010.

Commission Nationale de l'Informatique et Libertés (CNIL), Recommendations for companies planning to use Cloud computing services, not dated.

College Bescherming Persoonsgegevens, "Publicatie van Persoonsgegevens op het Internet", *CBP Richtsnoeren*, December 2007.

Data Protection Commissioner, "Report of Audit – Facebook Ireland Ltd.", 21 December 2011.

Agencia Espanalo de Protección de Datos, "Statement on Internet Search Engines", December 2007.

E. Denham (Assistant Privacy Commissioner of Canada), "Report of Findings into the complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act", 22 July 2009.

Office of the Privacy Commissioner of Canada, "PIPEDA - Processing Personal Data Across Borders Guidelines", 27 January 2009.

United States Federal Trade Commission (FTC), *In the matter of Facebook Inc. – Decision and Order*, Docket No. C-4365, 27 July 2012.

Garante per la protezione dei dati personali, Provvedimento dell'11 febbraio 2016 [doc. web n. 4833448], 11 Feburary 2016.

5 RECOMMENDATIONS AND DECLARATIONS

COUNCIL OF EUROPE

Parliamentary Assembly of the Council of Europe, Recommendation 509 (1968) concerning Human rights and modern scientific and technological developments, 31st January 1968 (16th Sitting).

Committee of Ministers of Council of Europe, Resolution (73)22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973 (224th meeting of the Ministers' Deputies).

Committee of Ministers of the Council of Europe, Resolution (74)29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974 (236th meeting of the Ministers' Deputies).

Committee of Ministers of the Council of Europe, Recommendation R(86)1 on the protection of personal data for social security purposes, 23 January 1986 (392nd meeting of the Ministers' Deputies).

Committee of Ministers of the Council of Europe, Recommendation R(99)5 for the protection of privacy on the internet, 23 February 1999 (660th meeting of the Ministers' Deputies).

Committee of Ministers of the Council of Europe, Declaration on freedom of communications on the Internet, 28 May 2003 (840th meeting of the Ministers' Deputies).

Project Group on Data Protection (CJ-PD) of the Council of Europe, Guiding principles for the protection of personal data with regard to smart cards, 12 May 2004 (adopted at the 79th Plenary the European Committee on Legal Co-operation (CDCJ).

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data of the Council of Europe, Opinion of the T-PD in the interpretation of the concepts of automatic processing and controller of the file in context of worldwide telecommunications networks, T-PD-BUR (2006) 08 E fin, Strasbourg, 15 March 2007.

Council of Europe, Recommendation of the Committee of Ministers to member States on the protection of human rights with regard to search engines, CM/Rec(2012)3, 4 April 2012 (adopted at the 1139th meeting of the Ministers' Deputies).

OECD

Organisation for Economic Co-operation and Development (OECD), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

Organisation for Economic Co-operation and Development (OECD), Declaration on Transborder Data Flows, 11 April 1985.

Organisation for Economic Co-operation and Development (OECD), Declaration on the Protection of Privacy in Global Networks, adopted at the Ottawa Ministerial Conference 7-9 October 1998, adopted as OECD Council Resolution on 19 October 1998.

Organisation for Economic Co-operation and Development (OECD), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, 12 June 2007.

Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.

Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, C(2015)115, 17 September 2015.

OTHER

International Working Group on Data Protection in Telecommunications, Report and Guidance on Privacy in Social Network Services – "Rome Memorandum", adopted 3-4 March 2008.

International Data Protection and Privacy Commissioners' Conference: Resolution on Privacy Protection and Search Engines, 28th edition, London, 2-3 November 2006.

International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum", adopted 23-24 April 2012.

6 DOCTRINE

MONOGRAPHS

Bainbridge, D., *EC Data Protection Directive*, London, Butterworths, 1996, 328 p.

Baldwin, R. and Cave, M., *Understanding regulation – Theory Strategy and Practice*, Oxford, Oxford university press, 1999, 363 p.

Bennett, C.J., *Regulating Privacy*, Ithaca, Cornell University Press, 1992, 263 p.

Boonk, M.L., *Zeker over zoeken? Naar een juridisch kader voor verichtingen van zoeksystemen met betrekking tot via internet beschikbare open content*, Zutphen, Uitgeverij Paris, 2013, 466 p.

Bygrave, L.A., *Data protection law: approaching its rationale, logic and limits*, The Hague, Kluwer Law International, 2002, 426 p.

Cannataci, J.A., *Privacy and Data Protection Law: International Development and Maltese Perspectives*, Oslo, Norwegian University Press, 1986, 239 p.

Coene, B. *De wenselijkheid van de investeringsbescherming geboden door de sui generis intellectuele rechten rond chips, computerprogramma's en databanken*, Proefschrift aangeboden tot het behalen van de titel van Doctor in de Rechten aan de KU Leuven en de UGent, Academiejaar 2015-2016, 3 February 2016, 935 p.

Dammann, U., Mallmann, O. and Simitis, S., (eds.), *Data Protection Legislation. An International Documentation. English – German*, 1977, Frankfurt am Main, Alfred Metzner Verlag GmbH, 203 p.

Dammann, U. and Simitis, S., *EG-Datenschutzrichtlinie*, 1997, Baden-Baden, Nomos Verlagsgesellschaft, 346 p.

De Bot, D., *Verwerking van Persoonsgegevens*, Kluwer, Antwerpen, 2001, 403 p.

De Bot, D., *Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart*, Brugge, Vandenbroele, 2005, 469 p.

D. De *Cock, Contributions to the Analysis and Design of Large-Scale Identity Management Systems*, Dissertation presented in partial fulfillment of the requirements for the degree of Doctor in Engineering, June 2011, 234 p.

De Hert, P., Gutwirth S. and Debeuckelaere, W., *Anthologie privacy: referentietekst*, published by Commissie voor de Bescherming van de Persoonlijke Levenssfeer, 2013, 93 p.

Demeyere, S., Samoy, I. and Stijns, S., *Aansprakelijkheid van een contractant jegens derden – De rechtspositie van de nauw betrokken derde*, Brugge Die Keure, 2015, 167 p.

Dierickx, L., "Recht op afbeelding" in X., Reeks *Instituut voor Familierecht en Jeugdrecht KU Leuven*, nr. 89, Antwerpen, Intersentia, 2005, 345 p.

Flaherty, D.H., *Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, & the United States*, 1989, Chapel Hill, The University of North Carolina Press, 483 p.

A.L. George, A.L. and Bennet, A., *Case Studies and Theory Development in the Social Sciences*, 2005, London, MIT Press, 331 p.

González Fuster, G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014, 284 p.

Gutwirth, S., *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002, 152 p.

Hensler, D.R., *Designing Empirical Legal Research: A Primer for Lawyers*, 2011, second revision, 145 p.

Hijmans, H., *The European Union as a constitutional guardian of internet privacy and data protection*, Academisch proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam en de Vrije Universiteit Brussel, 2016, 543 p.

Hondius, F. W., *Emerging data protection in Europe*, Amsterdam, North-Holland Publishing Company, 1975, 282 p.

Hutter, B.M., *Regulation and Risk. Occupational Health and Safety on the Railways*, Oxford, Oxford University Press, 2001, 356 p.

Jones, A. and Sufrin, B., *EU Competition Law – Texts, Cases and Materials*, Oxford, Oxford University Press, Fourth Edition, 2011, 1287 p.

Kayser, P., *La protection de la vie privée. Protection du secret de la vie privée*, Paris, Economica, 1984, 605 p.

Kosta, E., *Unravelling consent in European data protection legislation: a prospective study on consent in electronic communications*, Doctoral Thesis, Submitted 1 June 2011, 364 p.

Kuner, C., *European data protection law: corporate compliance and regulation*, 2nd edition, Oxford, Oxford University Press, 2007, 552 p.

Lievens E., *Protecting Children in the Digital Era – the Use of Alternative Regulatory Instruments*, Leiden, Martinus Nijhoff Publishers, International Studies in Human Rights, 2010, 584 p.

Marchini, R., *Cloud computing: A Practical Introduction to the Legal Issues*, London, BSI Standards Institution, 2010, 166 p.

Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., *Handbook of Applied Cryptography*, Boca Raton, CRC Press, 1997, 780 p.

Moerel, L., *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers*, Oxford, Oxford University Press, 2012, 354 p.

Newman, A., *Protectors of Privacy: Regulating personal data in a global economy*, 2008, New York, Cornell University, 221 p.

Niblett, G.B.F., "Digital information and the privacy problem", *OECD Informatics Studies*, nr. 2, 1971, Paris, OECD, 58 p.

Nugter, A.C.M., *Transborder Flow of Personal Data within the EC. A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector*, Deventer, Kluwer, Computer/Law Series n° 6, 1990, 430 p.

Oderkerk, A.E., *De preliminaire fase van het rechtsvergelijkend onderzoek*, Ph. D. Thesis, 1999, msterdam Center for International Law (ACIL), 484 p.

Overkleeft-Verburg, M., *De Wet persoonsregistraties - norm, toepassing en evaluatie*, Proefschrift ter verkrijging van de graad van doctor aan de Katholieke Universiteit Brabant, Hilvarenbeek, 1995, 607 p.

Solove, D.J., *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, 2007, New Haven, Yale University Press, 247 p.

Stijns, S., *Verbintenissenrecht*, Boek 1bis, Brugge, Die Keure, 2013, 152 p.

Thijssen, M.B.J., *De Wbp en de vennootschap*, Deventer, Kluwer, 2009, 342 p.

Tridimas, T., *The General Principles of EU Law*, 2nd edition, Oxford, Oxford University Press, 2006, 591 p.

Van Hoboken, J., *Search engine freedom. On the implications of the right to freedom of expression for the legal governance of Web search engines*, Academisch Proefschrift ter verkrijging van de graad van doctor aan de Universiteit van Amsterdam, defended on 23 March 2012, 357 p.

Vansweevelt, T. en Weyts, B., *Handboek Buitencontractueel Aansprakelijkheidsrecht*, Antwerpen, Intersentia, 2009, 935 p.

Vinge, P.G. , *Swedish Data Act*, Federation of Swedish Industries, No. 43, Stockholm, Svanbäck & Nymans Boktr., 1974 (original release: 1973), 22 p.

Yin, R.K., *Case Study Research – Design and Methods*, 2009, London, Sage Publications, Fourth Edition, 219 p.

Yin, R.K. Applications of Case Study Research, 2012, London, Sage Publications, Third Edition, 231 p.

Zhang, L., *Knowledge Graph Theory and Structural Parsing*, PhD Thesis, University of Twente, Twente University Press, 2002, 232 p.

Zittrain, J., *The Future of the Internet— And How to Stop It*, New Haven, Yale University Press, 2008, 342 p.

ARTICLES, BOOK CHAPTERS AND EDITED WORKS

Agre, P.E. and Rotenberg M. (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, 325 p.

Alhadeff, J., Van Alsenoy, B. and Dumortier, J., "The accountability principle in data protection regulation: origin, development and future directions", in D. Guagnin, L. Hempel, C. Ilten a.o. (eds.), *Managing Privacy through Accountability*, Houndmills (UK), Palgrave Macmillan, 2012, p. 49-82.

Aronstein, C., "Défense de la vie privée. Essai pour contribuer à la survie de notre civilisation", *Journal des Tribunaux* 1971, p. 453-463.

Ausloos, J. and Kuczerawy, A., "From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain ruling", *CiTiP Working Paper Series* 2015, 38 p.

Balboni, P. "Data Protection and Data Security Issues Related to Cloud Computing in the EU", in N. Pohlmann, H. Reimer and W. Schneider (eds.), *ISSE 2010 Securing Electronic Business Processes*, Springer, 2010, p. 163-172.

Bagherjeiran, A., Bhatt, R.P., Parekh, R. and Chaoji, V., "Online Advertising in Social Networks", in B. Furht (ed.), *Handbook of Social Network Technologies and Applications*, 2010, New York, Springer, p. 651-689.

Beer, D., "Social network(ing) sites … revisiting the story so far: A response to danah boyd & Nicole Ellison", *Journal of Computer-Mediated Communication* 2008, Vol. 13, p. 516–529.

Bender, J., "eIDAS regulation: eID – Opportunities and Risks", 25th SmartCard Workshop, 4-5 February 2015, p. 157-166.

Bing, J., "A Comparative Outline of Privacy Legislation", *Comparative Law Yearbook* 1978, Vol. 2, p. 149-181.

Bing, J., Forsberg, P. and Nygaard, E., "Legal problems related to transborder data flows", in OECD, *An Exploration of Legal Issues in Information and Communication Technologies*, Information Computer Communication Policy nr. 8, Paris, OECD, 1983, 135 p.

Bing, J., "The Council of Europe Convention and the OECD Guidelines on Data Protection", *Michigan Yearbook of International Legal Studies* 1984, Vol. 5, p. 271-303.

Bing, J., "Data Protection in a Time of Changes", in W.F. Korthals Altes a.o. (eds.), *Information law towards the 21st Century*, Information law series 2, Deventer, Kluwer Law and Taxation Publishers, 1992, p. 247-259.

Birnhack, M., "Reverse Engineering Information Privacy Law", *Yale Journal of Law and Technology* 2012, Vol. 24, p. 24-91.

Black, J., "The Rise, Fall and Fate of Principles Based Regulation", *LSE Law Society and Economy Working Papers* 17/2010, 2010, 26 p.

Blume, P., "Controller and processor: is there a risk of confusion?", *International Data Privacy Law* 2013, Vol. 3, No. 2, p. 140-145.

Blume, P., "An alternative model for data protection law: changing the roles of controller and processor", *International Data Privacy Law* 2015, Vol. 5, No. 4, p. 292-297.

Bocken, H., "Samenloop contractuele en buitencontractuele aansprakelijkheid", *NjW* 2007, nr. 169, p. 722-731.

Börjesson, M., "The Swedish Data Act in Transition", in P. Blume (ed.), *Nordic Studies in Information Technology and Law*, Computer/Law Series, Kluwer, 1991, p. 151-162.

Boulanger, M.-H. , De Terwangne, C. , Léonard, T., Louveaux, S., Moreau, D. and Poullet, Y., "La Protection des Données à caractère personnel en droit communautaire", *Journal de Tribunaux Droit Européen* 1997, p. 121-155.

Bovens, M., "Analysing and Assessing Accountability: A conceptual Framework", *European Law Journal* 2007, vol. 13, p. 946–967.

boyd, d. "Friendster and Publicly Articulated Social Networks", in *Conference on Human Factors and Computing Systems* (CHI 2004), Vienna, ACM, April 24–29, 2004, p. 1279-1282.

boyd, d.m. and Ellison, N.B., "Social Networking Sites: Definition, History and Scholarship", *Journal of Computer-Mediated Communication* 2008, vol. 13, p. 210-230.

Boyd, J. and Ingberman, D.E., "The 'Polluter pays principle': Should Liability be Extended When the Polluter Cannot Pay?", *The Geneva Papers on Risk and Insurance* 1996, Vol. 21, No. 79, p. 182-203.

Brugger, W., "Legal Interpretation, Schools of Jurisprudence, and Anthropology: Some Remarks from a German Point of View", *American Journal of Comparative Law* 1994, Vol. 42, No. 2, p. 395-421.

Buquicchio, G., "The work of the Council of Europe in the field of data protection", in Council of Europe, *Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection*, 1983, Rome, Camera dei Deputati, Annex I, p. 229-233.

Burkert, H. "Privacy - Data Protection A German/European Perspective", in C. Engel K.H. Keller (eds.), *Governance of Global Networks in the Light of Differing Local Values*, 2000, Baden-Baden, Nomos, p. 43-69.

Bygrave, L.A., "Core principles of data protection", *Privacy Law and Policy Reporter* 2001, vol. 7, issue 9, p. 169.

Callens, S., a.o. (ed.), *Chapters on pharmaceutical law*, Antwerpen, Intersentia, 2000, 194 p.

Campbell, D. and Fisher, J. (eds.), *Data transmission and privacy*, Center for International Legal Studies, Dordrecht, Martinus Nijhoff Publishers, 1994, 509 p.

Casteluccia, C., "Behavioural Tracking on the Internet: A Technical perspective", S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, 2013, Dordrecht, Springer Science+Business Media, p. 21-33.

Cate, F.H., "The EU Data Protection Directive, Information Privacy, and the Public Interest", *Iowa Law Review* 1995, 431-443.

Centrum voor Internationaal Strafrecht, "De Belgische privacy-wetgeving, een eerste analyse", *Rechtskundig Weekblad* 1992-1993, nr. 34, p. 1145-1154.

Chadwick, D., "Federated Identity Management", in Alessandro Aldini, Gilles Barthe and Roberto Gorrieri (eds.), *Foundations of Security Analysis and Design V*, FOSAD 2007/2008/2009 Tutorial Lectures, Springer, 2009, p. 96-120.

Claeys, I., "Buitencontractuele aansprakelijkheid van contractanten en hulppersonen? Als het contractuele evenwicht maar niet wordt verstoord", in S. Stijns (ed.), *Verbintenissenrecht*, Brugge, Die Keure, 2004, Reeks 'Themis', nr. 23, p. 27-42.

Cook, T., "The law relating to computer bureaux", in C. Edwards and N. Savage (eds), *Information Technology & The Law*, 1986, MacMillan Publishers, p. 159-167.

Cousy, H. and Droshout, D., "Fault under Belgian Law", in P. Widmer (ed.), Unification of Tort Law: Fault, 2005, The Hague, Kluwer Law International, p. 27-51.

Cousy, H. and Droshout, D., "Belgium", in B.A. Koch and H. Koziol (ed.), *Unification of Tort Law: Strict Liability*, 2002, The Hague, Kluwer International, p. 43-74.

Cousy, H. and Droshout, D., "Liability for Damage Caused by Others under Belgian Law", in J. Spier (ed.), *Unification of Tort Law: Liability for Damage Caused by Others*, The Hague, Kluwer law International, p. 37-54.

Cousy, H. and Droshout, D., "Multiple Tortfeasors under Belgian Law", in. W.V.H. Rogers (Ed.), *Unification of Tort Law: Multiple Tortfeasors*, The Hague, Kluwer Law International, 2004, p. 29-52.

Crook, A., "Data Protection in the United Kingdom, Part 2", *Journal of Information Science* 1983, Vol. 7, p. 47-57.

Cuijpers, C. and Schroers, J., "eIDAS as guideline for the development of a pan European eID framework in FutureID", *Open Identity Summit* 2014 vol. 237, p. 23-38.

de Andrade, N.N.G., "'Electronic Identity for Europe': Moving from Problems to Solutions", *Journal of International Commercial Law and Technology* 2013, Vol. 8, No.2, p. 104-109.

de Azevedo Cunha, M.V., Marin, L. and Sartor, G., "Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web", *International Data Privacy Law* 2012, Vol. 2, No. 2, p. 50-67.

De Boeck, A., "Aansprakelijkheid voor gebrekkige dienstverlening", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Kluwer, 2008, looseleaf.

De Bot, D., "Art. 15bis Wet Persoonsgegevens", in X., *Personen- en familierecht. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2001, looseleaf.

De Cock, D., Van Alsenoy, B., Preneel, B. and Dumortier, J. "The Belgian eID Approach", in W. Fumy and M. Paeschke, *Handbook of eID Security. Concepts, Practical Experiences, Technologies*, 2011, Erlangen, Publicis, p. 117-139.

Defreyne, E. and Romain, R., "L'arrêt « Google Spain » : commentaire et mise en perspective", *Revue du Droit des Technologies de l'Information* 2014, n° 56, p. 73-114.

De Groef, W., Devries, D., Reynaert, T. and Piessens, F., "Security and Privacy of Online Social Network Applications", in L. Caviglione, M. Coccoli and A. Merlo (eds.), *Social Network Engineering for Secure Web Data and Services*, IGI Global, 2013, p. 206-221.

De Hert, P., "Een betere bescherming van de privacy door de nieuwe wet verwerking persoonsgegevens? Analyse van nieuwigheden en tekortkomingen", in X., *CBR Jaarboek 2000-2001*, Antwerpen, Maklu, 2001, 365-409.

De Hert, P. and Gutwirth, S. "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law*, Antwerpen/Oxford, Intersentia, 2006, p. 61-104.

De Hert, P. and Gutwirth, S. "Data Protection and the Case Law of Strasbourg and Luxemburg: Constitutionalism in Action", in S. Gutwirth, Y. Poullet, P. De Hert, J. Nouwt and C. De Terwangne (eds.), *Reinventing data protection?*, Dordrecht, Springer Science, 2009, p. 3-44.

De Hert, P., Papakonstantinou, V. and Kamara, I., "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection", *Brussels Privacy Hub Working Paper*, Vol. 1, No. 2, November 2014, 26 p.

De Hert, P. and Papakonstantinou, V., "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review* 2012, vol. 28, p. 130-142.

De Hert, P. and Papakonstantinou, V., "Comment – Google Spain -Addressing Critiques and Misunderstandings One Year Later", *Maastricht Journal of European and Comparative Law* 2015, Vol. 22, No. 4, p. 624-638.

De Hert P. and Saelens, R., "Recht op afbeelding", *TPR* 2009, afl. 2, p. 867-917.

Determann, L., "Data Privacy in the Cloud—Myths and Facts", *Institute for IT Law*, 10 April 2012, online publication at http://www.iitr.us/publications/40-data-privacy-in-the-cloud-a-dozen-myths-and-facts.html.

Dirix, E., "Aansprakelijkheid van en voor hulppersonen", in. M. Storme (ed.), *Recht Halen uit Aansprakelijkheid*, Gent, Mys & Breesch, 1993, p. 342.

Docquir, B., "Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au coeur de la relation contractuelle", *Revue de Droit Commercial* 2011, Vol. 10, p. 1000-1015.

Dumortier, J., "Privacybescherming en gegevensverwerking. Aantekeningen bij de Wet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens", *Vlaamse Jurist* 1993, p. 4-14.

Dumortier, J. and Vandezande, N., "Trust in the proposed EU regulation on trust services?", *Computer Law and Security Review* 2012, Vol. 28, p. 568-576.

Dworkin, G., "The Younger Committee Report on Privacy", *The Modern Law Review* 1973, Vol. 36, No. 4, p. 399-406.

Edwards, C. and Savage, N., "Data Privacy: the UK Experience", in C. Edwards and N. Savage (eds), *Information Technology & The Law*, Basingstoke, MacMillan Publishers, 1986, p. 75-142.

Ehrleich, I. and Posner, R. A., "An Economic Analysis of Legal Rulemaking", *The Journal of Legal Studies* 1974, Vol. 3, No. 1, p. 257-286.

Enders, A., Hungenberg, H., 'The long tail of social networking. Revenue models of social networking sites", *European Management Journal* 2008, Vol. 26, p. 199-211.

Erdos, D., "Filling Defamation's Gaps: Data Protection and the Right to Reputation", *Oxford Legal Studies Research Paper* 2013, No. 69, 41 p.

Esayas, S.Y., "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *Computer, Law & Security Review* 2012, Vol. 28, p. 662-678.

Evans, A.C., "Data Protection Law", *The American Journal of Comparative Law* 1981, vol. 29, no. 4, p. 571-582.

Fang, Z., "E-Government in Digital Era: Concept, Practice, and Development", *International Journal of The Computer, The Internet and Management* 2002, Vol. 10, No.2, p. 1-22.

Fon, V. and Parisi, F., "Codifications and the optimal specificity of legal rules", Law and Economics Working Paper Series 04-32, *George Mason University School of Law*, 2007, 22 p.

Freese, J., "The Swedish Data Act", *Current Sweden* 1977, No. 178, p. 1-8.

Fuster, G.G., De Hert, P. and Gutwirth, S., "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology* 2008, Vol. 22, p. 191-202.

Garcia, F.J., "Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators", *Fordham Intell. Prop. Media & Ent. L.J.* 2005, Vol. 15, p. 1204-1243.

Garcia, S.S. , Oliva, A.G., Belleboni, E.P. and De La Cruz, I.P., "Current Trends in Pan-European Identity Management Systems", *IEEE Technology and Society Magazine* 2012, Vol. 31, Issue 3, p. 1204-1243.

Garrie, D.B., Duffy-Lewis, M., Wong, R. and Gillespie, R.L., "Data Protection: the Challenges Facing Social Networking", *International Law & Management Review* 2010, Vol. 6, p. 127-152.

Gellert, R., "Understanding data protection as risk regulation", *Journal of Internet Law* 2015, p. 3-16.

Gelman, L., "Privacy, Free Speech, and "Blurry-Edged" Social Networks", *Boston College Law Review* 2009, vol. 50, p. 1315-1344.

Gilbert, F., "Cloud service providers as joint-data controllers", *Journal of Internet Law* 2011, p. 3-13.

Godin, B., "The information economy: the history of a concept through its measurement, 1949-2005", *History and Technology: An International Journal* 2008, Vol. 24, n. 3, p. 255-287.

Goettke, R. and Christiana, J., "Privacy and Online Social Networking Websites", Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, May 14, 2007. http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf.

Grimmelmann, J., "Speech engines", *Minnesota Law Review* 2014, Vol. 98, p. 868-952.

Grönlund, A. and Horan, T.A., "Introducing e-Gov: history, definitions and issues", *Communications of the Association for Information Systems* 2004, Vol. 15, p. 713-729.

Gross, R. and Acquisti, A., "Information Revelation and Privacy in Online Social Networks", in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (WPES'05), Virginia, 2005, p. 71-80.

Guiliams, S., "Eenzelfde schade of andere schade bij pluraliteit van aansprakelijken", *Nieuw Juridisch Weekblad* (NJW) 2010, afl. 230, p. 699-700.

Guiliams, S., "De verdeling van de schadelast bij samenloop van een opzettelijke en een onopzettelijke fout", *Rechtskundig Weekblad* (R.W.) 2010-2011, nr. 12, p. 474-485.

Gutwirth, S., "De toepassing van het finaliteitsbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens", *Tijdschrift voor Privaatrecht* 1993, vol. 4, p. 1409-1477.

Harris, E.C., "Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have All the Answers", *Am. U. Int'l L. Rev.* 2007, Vol. 22, p. 745-799.

Hartzog, W. and Stutzman, F., "The Case for Online Obscurity", *California Law Review* 2013, Vol. 101, No. 1, p. 1-49.

Heidemann, J., Klier, M. and Probst, F., "Online social networks: A survey of a global phenomenon", *Computer Networks* 2012, vol. 56, p. 3866–3878.

Helberger, N. and Van Hoboken, J., "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers", *Computer Law Review International* (Cri) 2010, Vol. 4, p. 101-109.

Heyman, R. and Pierson, J., "An Explorative Mapping of the Belgian Social Media Value Network and its Usage of Personal Identifiable Information", in M. Hansen a.o. (eds.), *Privacy and Identity*, IFIP, AICT, 2013, p. 203-213.

Hijmans, H., "Right to Have Links Removed - Evidence of Effective Data Protection", *Maastricht Journal of European and Comparative Law* 2014, Vol. 21, No. 3, p. 555-563.

Hildebrandt, M. and Koops, B.J., "The Challenges of Ambient Law and Legal Protection in the Profiling Era", *The Modern Law Review* 2010, p. 428-460.

Holleaux, A., "La loi du 6 Janvier 1978 sur l'informatique et les libertés (I) ", *La Revue Administrative* 1978, Vol. 31, n° 181, p. 31-40.

Holleaux, A., "La loi du 6 Janvier 1978 sur l'informatique et les libertés (II) ", *La Revue Administrative* 1978, Vol. 32, n° 182, p. 160-165.

Hornung, G., "A General Data Protection Regulation for Europa? Light and Shade in the Commission's Draft of 25 January 2012", *Scripted* 2012, Volume 9, Issue 1, p. 64-81.

Huber, M., Mulazzani, M., Schrittwieser, S., Weippl, E.R., "AppInspect – Large-scale Evaluation of Social Apps", *Proceedings of ACM Conference on Online Social Networks* (CSON) 2013, p. 143 – 154.

Hustinx, H., "Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations", speech delivered at the 11th Conference on Data Protection and Data Security, Berlin, 8 June 2009.

Hustinx, P., European Data Protection Supervisor, Data protection and Cloud Computing under EU law, speech delivered at the Third European Cyber Security Awareness Day, European Parliament, 13 April 2010.

Ilshammar, L., "When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s", *HUMAN IT* 2007, Vol. 9, No. 1, p. 6-37.

Itzcovich, G. "The Interpretation of Community Law by the European Court of Justice", *German Law Journal* 2009, Vol. 10, No. 5, p. 537-560.

Jacobs, F.G., "Recent Development in the Principle of Proportionality in European Community Law", in E. Ellis (ed.), *The Principle of Proportionality in the Laws of Europe*, 1999, Hart Publishing, Oxford, p. 1-22.

Joint, A. and Baker, E. "Knowing the past to understand the present – issues in the contracting for cloud based services", *Computer Law & Security Review* 2011, Vol. 27, p. 407-415.

Källner, C.G., "Personal Data: The Open Access Approach", in OECD, *Policy issues in data protection and privacy. Concepts and perspectives*, Proceedings of the OECD Seminar 24th-26th June 1974, Paris, OECD Informatics Studies, no. 10, 1976, p. 59-65.

Kaplow, L., "Rules versus Standards: An Economic Analysis", *Duke Law Journal* 1992, Vol. 42, p. 557-629.

Karst, K.L., "'The Files': Legal Controls over the Accuracy and Accessibility of Stored Personal Data', *Law and Contemporary Problems* 1966, vol. 31, no. 2, 342-376.

Kestemont, L., "Methods for traditional legal research, Reader Research Master in Law: Methods of Legal Research", KU Leuven - University of Tilburg (Leuven/Tilburg), 2015, 36 p.

Kestemont, L., "A typology of research objectives in legal scholarship", *Electronic Supplement to the Russian Juridical Journal* 2015, Vol. 5, p. 5-21.

Keuleers, E. and Dinant, J.M., "Multi application smart card schemes - Data protection: multi-application smart cards: the use of global unique identifiers for crossprofiling purposes – Part I", *Computer Law and Security Report* 2003, vol. 19, no. 6, p. 480-486.

Kirby, M.D., "Transborder Data Flows and the 'Basic Rules' of Data Privacy", *Stanford Journal of International Law* 1980, Vol. 16, no. 42, p. 27-66.

Kirby, M. "The history, achievement and future of the 1980 OECD guidelines on privacy", *International Data Privacy Law* 2011, Vol. 1, No. 1, 6-14.

Ko, M.N., Cheek, G.P. and Shebab, M., "Social-Networks Connect Services", *Computer* 2010, Issue n° 8, IEEE Computer Society, p. 37-43.

Kohl, U. "Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)", *International Journal of Law and Information Technology* 2013, p. 1-48.

Koops, B.J., "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be Forgotten" in Big Data Practice", *Scripted* 2011, Vol. 8, Issue 3, p. 229-256.

Kontaxis, G., Polychronakis, M., Keromytis, A.D. and Markatos, E.P., "Privacy-Preserving Social Plugins", *Proceedings of the 21st USENIX conference on Security symposium*, 2012, 16 p.

Koppell, J., "Pathologies of Accountability: ICANN and the Challenge of "Multiple accountabilities Disorder"", *Public Administration Review* 2005, Vol. 65, Issue 1, p. 94-108.

Korobkin, R.B., "Behavioural analysis and legal form: Rules vs. Standards Revisited", *Oregon Law Review* 2000, Vol. 79, No. 1, p. 23-58.

Kosta, E. and Dumortier, J., "The Data Retention Directive and the principles of European Data protection legislation", *Medien und Recht International* 2007, Issue 3, p. 130-136.

Kosta, E. Zibuschka, J., Scherner, T. and Dumortier, J., "Legal considerations on privacy-enhancing Location Based Services using PRIME technology", *Computer, Law & Security Review* 2008, Vol. 24, p. 139-146.

Kosta, E., Kalloniatis, C. , Mitrou, L. and Kavakli, E., "Search Engines: Gateway to a New "Panopticon"?", in S. Fischer-Hübner a.o. (eds.), *Trust, Privacy and Security in Digital Business*, Lecture Notes in Computer Science Volume 5695, 2009, p. 11-21.

Kosta, E., Kalloniatis, C., Mitrou, L. and Gritzalis, S., "Data protection issues pertaining to social networking under EU law", *Transforming Government: People, Process and Policy* 2010, Vol. 4, No. 2, p. 193-201.

Krishnamurthy, B., and Wills, C.E., "Characterizing Privacy in Online Social Networks", WOSN 2008, *Proceedings of the 1st ACM workshop on Online social networks*, 2008, p. 37-42.

Krishnamurthy, B. and Wills, C.E., "On the Leakage of Personally Identifiable Information Via Online Social Networks", WOSN 2009, *Proceedings of the 2nd ACM workshop on Online social networks*, 2009, p. 7-12.

Kuan Hon, W., Millard, C. and Walden, I., "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", Queen Mary University of London, School of Law, Legal Studies Research Paper No. 77/2011, 31 p.

Kuczerawy, A. and Coudert, F., "Privacy Settings in Social Networking Sites: Is It Fair?", in S. Fischer-Hübner et al. (eds.): *Privacy and Identity Management for Life*, 2011, p. 231-243.

Kuner, C., "Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies", *Privacy & Security Law Report* 2008, vol. 07, no. 44, p. 1-5.

Kuner, C., "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", *TILT Law & Technology Working Paper Series*, 2010, 90 p.

Kuner, C. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", Bloomberg BNA, *Privacy and Security Law Report*, 2 June 2012, p. 1-15.

Lando, O. and Beale, H. (eds.), *Principles of European Contract Law - Parts I and II*, prepared by the Commission on European Contract Law, The Hague, Kluwer Law International, 2000, 610 p.

Lauvaux, M., "De burgerlijke aansprakelijkheid van werknemers", *Oriëntatie* (Or.) 2005, afl. 3, p. 65-75.

Layton, C. "Protection of Privacy – Future Prospects at the European Communities Level", in OECD, "Transborder Data Flows and the Protection of Privacy", Information Computer Communications Policy, nr. 1, 1979, Paris, OECD, p. 213-216.

Leenes, R., "Who Controls the Cloud?", *Revista D'Internet, Dret I Política* (IDP) 2010, nr. 11, p. 1-10.

Leitold, H. and Zwattendorfer, B., ""STORK: Architecture, Implementation and Pilots", in N. Pohlmann a.o. (eds.), *ISSE 2010 Securing Electronic Business Processes*, Springer, 2010, p. 131-142.

Lenoir, N., "La loi 78-17 du 6 janvier 1978 et la Commission national de l'informatique et des liberté: Éléments pour un premier bilan de cinq années d'activité", *La Revue administrative* 1983, Vol. 36, no. 215, p. 451-466.

Léonard, T., and Poullet, Y., "La protection des données à caractère personnel en pleine (r)évolution", *J.T.* 1999, p. 377-396.

Léonard, T., "La protection des données à caractère personnel et l'entreprise", in X., *Guide juridique de l'entreprise*, Brussels, Kluwer, 2004, livre 112.1, pp. 9-64.

Léonard, T. and Mention, A., "Transferts transfrontaliers de données: quelques considérations théorique et pratiques", in B. Docquir and A. Puttemans (eds.), *Actualités du droit de la vie privée*, Bruylant, Bruxelles, 2008, p. 98-137.

Lynskey, O., "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez", *The Modern Law Review* 2015, Vol. 78, no. 3, p. 522-548.

Mahler, T., "Defining legal risk", paper presented at the conference "Commercial Contracting for Strategic Advantage – Potentials and Prospects", Turku University of Applied Sciences, 2007, 31 p.

Mantelero, A., "Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *European Journal for Law and Technology* 2012, Vol. 3, No. 2, 6 p.

Mayer-Schönberger, V., "Generational Development of Data Protection in Europe", in P.E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape*, 1998, London, MIT Press, 219-241.

MacCormick, N., "Argumentation and Interpretation in Law", *Ratio Juris* 1993, Vol. 6, No. 1, p. 16-29.

Marston, S. a.o., "Cloud computing — The business perspective", Decision Support Systems 2011, Vol. 51, p. 176-189.

McBride, J., "Citizen's Privacy and Data Banks: Enforcement of the Standards in the Data Protection Act 1984 (U.K.)", *Les Cahiers de Droit* 1984, vol. 25, n° 3, p. 533-552.

Merchant, K.A. and Otley, D.T., "A Review of the Literature on Control and Accountability", in C. S. Chapman, A. G. Hopwood and M. D. Shields (eds.), *Handbook of Management Accounting Research*, Vol. 2, 2007, Amsterdam, Elsevier, p. 785-802.

Miller, A.R., "Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society", *Michigan Law Review* 1969, vol. 67, p. 1089-1246.

Moerel, L. ,"The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 28-46.

Moerel, L., "Back to basics: when does EU data protection law apply?", *International Data Privacy Law* 2011, Vol. 1, No. 2, p. 92-110.

Montéro, E. "Les responsabilités liées au web 2.0", *Revue du Droit des Technologies de l'Information* 2008, n° 32, p. 363-388.

Mulgan, R., "'Accountability': an ever-expanding concept?", *Public Administration* 2000, vol. 78, No. 3, p. 55-573.

Mustonen, J. (ed.), The World's First Freedom of Information Act. Anders Chydenius' Legacy Today, Anders Chydenius Foundation's Publications 2, 2006, 103 p.

Odudu, O. and Bailey, D., "The single economic entity doctrine in EU competition law", *Common Market Law Review* 2014, Vol. 51, p. 1721-1758.

Olsen, T. and Mahler, T., "Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II", *Computer, Law & Security Review* 2007, Vol. 23, n° 5, p. 415-426.

Onstad, P.C., "Data Processing Services and Transborder Data Flows, in OECD, *Transborder Data Flows and the Protection of Privacy*, Proceedings of a Symposium held in Vienna, Austria, 20th-23rd September 1977, Paris, OECD, 1979,p. 178-182.

Pagano, R., "Panorama of Personal Data Protection Laws", in Council of Europe, Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection, 1983, Rome, Camera dei Deputati, Annex II, p. 236-348.

Pallis, G., Zeinalipour-Yazti, D. and Dikaiakos, M.D. in Vakali, A. and Jain, L.C. , (eds.), "Online Social Networks: Status and Trends", *New Directions in Web Data Management, Studies in Computational Intelligence* 2011, Vol. 331, Berlin, Springer-Verlag, p. 213-234.

Papakonstantinou, V., "A data protection approach to data matching operations among public bodies", *International Journal of Law and Information Technology* 2001, vol. 9, issue 1, 2001, 39-64.

Patrick, P.H., "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines", *Jurimetrics Journal* 1980-1981, Vol. 21, p. 405-420.

Peguera, M. "The Shaky Ground of the Right to Be Delisted", (Draft, August 2015, forthcoming in Vanderbilt Journal of Entertainment & Technology Law), 52 p., available at http://ssrn.com/abstract=2641876.

Peterson, H.E. and Turn, R., "System implications of information privacy", in *Proceeding AFIPS '67*, (Spring) Proceedings of the April 18-20, 1967, spring joint computer conference, ACM, New York, p. 291-300.

Raitio, J., "The Expectation of Legal Certainty and Horizontal Effect of EU Law", in U. Bernitz, X. Groussot and F. Schulyok (eds.), *General Principles of EU Law and European Private Law*, 2013, Croyden, Kluwer Law International, p 199-212.

Reed, C., "The Law of Unintended Consequences – Embedded Business Models in IT Regulation", *Journal of Information Law and Technology* 2007, vol. 2, p. 1-34.

Reich, N., "The Principle of Effectiveness and EU Private Law", in U. Bernitz, X. Groussot and F. Schulyok (eds.), *General Principles of EU Law and European Private Law*, 2013, Croyden, Kluwer Law International, p. 301-326.

Reid, E., "Liability for Dangerous Activities: A Comparative Analysis", *The International and Comparative Law Quarterly* 1999, Vol. 48, No. 4, p. 731-756.

Robben, F., "Toepassingsgebied en begripsdefinities", in J. Dumortier en F. Robben, Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer, Brugge, Die Keure, 1995, p. 20-61.

Rodotà, S., "Data Protection – Some problems for Newcomers", in Council of Europe, Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection, 1983, Rome, Camera dei Deputati, p. 186-193.

Roosendaal, A., "Facebook tracks and traces everyone: Like this!", *Tilburg Law School Legal Studies Research Paper Series*, No. 03/2011, 10 p.

Roosendaal, A.P.C., "We Are All Connected to Facebook … by Facebook!", in S. Gutwirth et al. (eds), *European Data Protection: In Good Health?*, Dordrecht, Springer, 2012, p. 3-19.

Roth, P. "Data Protection Meets Web 2.0 – Two Ships Passing in the Night", *UNSW Law Journal* 2010, Vol. 33, p. 532-561.

Salom, J.A., "'A third party to whom data are disclosed': A third group among those processing data", *International Data Privacy Law* 2014, Vol. 4, No. 3, p. 177-188.

Samyn, B., "Raad van Bestuur", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Wolters Kluwer, 2000-, looseleaf.

Sancho-Villa, D., "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten", *Legal Issues of Economic Integration* 2015, Vol. 42, no. 4, p. 357-381.

Sartor, G., "Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?", *International Data Privacy Law* 2013, Vol. 3, No. 1, p. 3-12.

Sartor, G. "Search Engines as Controllers – Inconvenient implications of a Questionable Classification", *Maastricht Journal of European and Comparative Law* 2014, Vol. 21, No. 3, p. 564-575.

Sayaf, R. and Clarke, D., "Access control models for online social networks", in L. Caviglione, Coccoli, M. and Merlo, A. (eds.) *Social Network Engineering for Secure Web Data and Services*, Hershey, IGI, 2013, p. 32-56.

Schmidtchen, D. a.o., "The Internalisation of External Costs in Transport: From the Polluter Pays to the Cheapest Cost Avoider Principle", *CSLE discussion paper series*, No. 2007-03, 2007, 157 p.

Schmidl, M., "The Challenges of Subprocessing and Suggested Solutions under German and EU Privacy Law", *Bloomberg BNA World Data Protection Report* 2013, Vol. 13, No. 2, p. 1-5.

Schneier, B., "A Taxonomy of Social Networking Data", *Security & Privacy* 2009, IEEE, Vol. 8, Issue 4, p. 88.

Schwartz, P. "Information Privacy in the Cloud", *University of Pennsylvania Law Review* 2013, Vol. 161, p. 1623-1662.

Seawright, J. and Gerring, J. "Case Selection Techniques in Case Study Research – A Menu of Qualitative and Quantitative Options", *Political Research Quarterly* 2008, Vol. 61, No. 2, p. 294-308.

Seipel, P., "The Right to Know - Computers and Information Power", in P. Blume (ed.), *Nordic Studies in Information Technology and Law*, Computer/Law series n° 7, Deventer, Kluwer, 1991, p. 7-43.

Sethi, N., "Reimagining Regulatory Approaches: on the Essential Role of Principles in Health Research Regulation", *Scripted 2015*, Vol. 12, Issue 2, p. 91-116.

Simitis, S., "Establishing Institutional Structures to Monitor and Enforce Data Protection", in OECD, "Policy issues in data protection and privacy. Concepts and perspectives", *OECD Informatics Studies*, nr. 10, Paris, OECD, 1976, p. 83-94.

Simitis, S., "Zwanzig Jahre Datenschutz in Hessen – eine kritische Bilanz", *Hessischer Landtag*, Neunzehnter Tätighkeitsbericht des hessischen Datenshutzbeauftragten, 1990, Drucksache 12/7651, p. 68-75.

Simitis, S., "Datenschutz", in H. Meyer and M. Stolleis (eds.), *Staats- und Verwaltungsrecht für Hessen*, 1996, fourth edition, Baden-Baden, Nomos Verlagsgesellschaft, p. 109-146.

Simitis, S., (ed.), *Kommentar zum Bundesdatenschutzgesetz*, 5th edition, Baden-Baden, Nomos Verlagsgesellschaft, 2003, 1623 p.

Simitis, S. "Privacy – An Endless Debate?", *California Law Review* 2010, Vol. 98, Issue 6, p. 1989-2005.

Sinclair, A., "The Chameleon of Accountability: Forms and Discourses", *Accounting, Organisations and Society* 1995, Vol. 20, p. 219-237.

Sjöblom, G., "Control in the History of Computing: Making an Ambiguous concept Useful", *IEEE Annals of the History of Computing* 2011, p. 86-870.

Solove, D., "A taxonomy of privacy", *University of Pennsylvania Law Review* 2006, Vol. 154, No. 3, p. 477-560.

Stadler, G., and Herzog, T., "Data Protection: International Trends and the Austrian Example", Guest Seminar at the International Institute for Applied Systems analysis, Laxenburg, Austria, 1981, 28 p.

Svantesson, D. and Clarke, R., "Privacy and consumer risks in cloud computing", *Computer Law & Security Review* 2010, Vol. 26, p. 391-397.

Svenonius, P., "Address", OECD, *Policy issues in data protection and privacy. Concepts and perspectives*, OECD Informatics Studies, nr. 10, 1976, OECD, Paris, p. 48

Tene, O., "What Google Knows: Privacy and Internet Search Engines", *Utah Law Review* 2008, no. 4, p. 1433-1492.

Tene, O., "Privacy: The new generations", *International Data Privacy Law* 2011, Vol. 1, No. 1, p.15-27.

Thijssen, M.B.J., "Data Protection and group companies", 17th BILETA Annual Conference April 5th - 6th, 2002, 12 p.

Thompson, M. "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries", *University of Hong Kong Faculty of Law Research Paper* No. 2015/45, 55 p.

Treacy, B. C. "Lessons from SWIFT: the 'controller' v 'processor' dilemma", *Complinet* 2008, 3 p.

Treacy, B., "Working Party confirms 'controller' and 'processor' distinction", *Privacy & Data Protection Journal* 2010, Vol. 10, Issue 5, p. 3-5.

Treacy, B., "Challenging times ahead for data processors", *Privacy & Data Protection Journal* 2012 Vol. 12, Issue 7, p. 3-6.

Tsormpatzoudi, P. and Coudert, F., "Technology providers' responsibility in protecting privacy… dropped from the sky?", *Paper presented at the Amsterdam Privacy Conference (APC)*, 23-26 October 2015, 13 p.

Turn, R. and Ware, W.H., "Privacy and Security Issues in Information Systems", *IEEE Transactions on Computers* 1976, Vol. C-25, No. 12, 1353-1361.

Turn, R., "Data security: costs and constraints" in OECD, *Policy issues in data protection and privacy. Concepts and perspectives*, *OECD Informatics Studies*, 1976, nr. 10, OECD, Paris, p. 243-265.

Van Alsenoy, B., Ballet, J., Kuczerawy, A. and Dumortier, J., "Social networks and web 2.0: are users also bound by data protection regulations?", *Identity in the information society* 2009, Vol. 2, n°1, p. 65-79.

Van Alsenoy, B., De Cock, D., Simoens, K., Dumortier, J. and Preneel, B., "Delegation and digital mandates: Legal requirements and security objectives", *Computer, Law and Security Review* 2009, Vol. 25, no 5, p. 415-431.

Van Alsenoy, B., "Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC", *Computer Law & Security Review* 2012, Vol. 28, p. 25-43.

Van Alsenoy, B., Kindt, E. and Dumortier, J., "Privacy and data protection aspects of e-government identity management", in S. Van der Hof, M.M. Groothuis (eds.), *Innovating Government - Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series (IT & Law), Vol. 20, T.M.C. Asser Press, Springer, 2011, p. 251-282.

Van Alsenoy, B., Kuczerawy A., and Ausloos, J., "Search Engines after *Google Spain*: Internet@Liberty or Privacy@Peril?", *ICRI Working Paper Series*, Working paper 15/2013, September 2013, 74 p.

Vandenberghe, H., "Aansprakelijkheid van de aansteller", *Tijdschrift voor Privaatrecht* (TPR) 2011, afl. 2, p. 575-612.

van der Sloot, B., "Welcome to the Jungle : the Liaiblity of Internet Intermediaries for Privacy Violations in Europe", *JIPITEC* 2015, Vol. 6, p. 211-228.

van der Wees, J.G.L., "De verantwoordelijke en de bewerker in de cloud", *Computerrecht* 2011, Afl. 3, p. 108-114.

Van Eecke, P., "Online service providers and liability: a plea for a balanced approach", *Common Market Law Review* 2011, Vol. 48, p. 1455-1502.

Van Eecke P. and Truyens, M., "Privacy and social networks", *Computer, Law & Security Review* 2010, Vol. 26, n° 5, p. 535-546.

Van Gyseghem, J.M., "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *Revue du Droit des Technologies de l'Information* 2011, vol. 42, p. 35-50.

Vegleris, P., "Preadvies" in X., *Privacy en de rechten van de mens. Handelingen van het Derde Internationaal Colloquium over het Europees Verdrag tot Bescherming van de Rechten van de Mens,* Leuven, Acco, 1974, p. 337-342.

Waters, R.D., Burnett, E., Lamm, A. and Lucas, J., "Engaging stakeholders through social networking: How nonprofit organisations are using Facebook", *Public Relations Review* 2009, Vol. 35, Issue 2, p. 102-106.

Witting, C., "Breach of the non-delegable duty: defending limited strict liability in tort", *University of New South Wales Law Journal* 2006, Vol. 29, No. 3, p. 33-60.

Wojtan, B., "The new EU Model Clauses: One step forward, two steps back?", *International Data Privacy Law* 2011, Vol. 1, No. 1, p. 76-80.

Wong, K, "Data Protection Law", *Data Processing* 1984, Vol. 26, no. 1, p. 34-37.

Wong, R., "The Shape of Things to Come: Swedish Developments on the Protection of Privacy", *SCRIPT-ed* 2005, Vol. 2, Issue 1, p. 107-124.

Wong, R. and Savirimuthu, J., "All or Nothing: This is the Question? The Application of Article 3(2) Data Protection Directive 95/46/EC to the Internet", *The John Marshall Journal of Information Technology and Privacy Law* 2008, Vol. 25, Issue 2. p. 241-266.

R. Wong, "Social Networking: Anybody is a Data Controller!", (last revised) 2008, 16 p. published online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1271668

R. Wong, "Social networking: a conceptual analysis of a data controller", *Communications Law* 2009, Vol. 14, No. 5, p. 142-149.

Wynant, L., "Aansprakelijkheid voor en van derden die voor de vennootschap werken: Personeel ter beschikking stellen van werknemers, onderaannemers", in X., *Bestendig Handboek Vennootschap & Aansprakelijkheid*, Mechelen, Wolters Kluwer, 2000-, looseleaf.

Xanthoulis, N., "Negotiating the EU Data Protection Reform: Reflections on the Household Exemption", in A. B. Sideridis a.o. (eds*.), E-Democracy, Security, Privacy and Trust in a Digital World*, 5th International Conference, E-Democracy 2013, Springer, Communications in Computer and Information Science, 2014, p. 135-152.

J. Zittrain, "Privacy 2.0", *University of Chicago Legal Forum* 2008, No. 1, article 3, p. 65-119.

REPORTS BY (INTER)GOVERNMENTAL BODIES

- *Council of Europe*

Council of Europe, Explanatory Report accompanying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS. 108, paragraph 13, available at http://conventions.coe.int/treaty/en/Reports/Html/108.htm.

Council of Europe, Legislation and Data Protection. Proceedings of the Rome Conference on problems relating to the development and application of legislation on data protection, 1983, Rome, Camera dei Deputati, 356 p.

- *European Union*

Commission des Communautés Européens, "Systèmes à grande puissance de traitement automatique de l'information. Besoins et applications dans la Communauté européenne et au Royaume-Uni vers les années soixante-dix", *Études, Série Industrie* 1971, n° 6, 64 p.

European Commission, First Report on the Application of Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21 November 2003, 25 p., available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0702&from=EN.

European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), 2010, 17 p. available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

European Commission, Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11 January 2012 SEC(2011) 1641 final, 141 p., available at http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1641_en.pdf.

European Commission, The Internal Market Information (IMI) System User Handbook, Update 2012, Publications Office of the European Union, Luxembourg, 2012, 64 p., available at http://ec.europa.eu/internal_market/imi-net/_docs/library/user_handbook_en.pdf.

European Commission, Directorate-General Informatics, "EU activities in the field of eID interoperability", December 2013, 3 p., available at http://ec.europa.eu/isa/documents/eu-activities-in-the-field-of-eid-interoperability.pdf.

European Commission, "Data protection guidelines for IMI users", not dated, 6 p., available at http://ec.europa.eu/internal_market/imi-net/docs/data_protection/data_protection_guidelines_en.pdf.

European Commission, "IMI roles and responsibilities", not dated, 6 p., accessible at http://ec.europa.eu/internal_market/imi-net/_docs/training/roles_responsibilities_en.pdf.

European Commission, Managing my authority and users, not dated, accessible at http://ec.europa.eu/internal_market/imi-net/_docs/training/managing_authority_users_en.pdf

European Union Agency for Fundamental Rights (FRA) and Council of Europe, *Handbook on European Data Protection Law*, 2014, 203 p., available at http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

European Commission, Introduction to the Connecting Europe Facility eID building block, Version 1.01, 2015, 34 p., accessible at https://joinup.ec.europa.eu/sites/default/files/introduction_to_the_connecting_europe_facility_eid_building_block_v1_01_0.pdf.

European Parliamentary Research Service (EPRS), "eGovernment – Using technology to improve public services and democratic participation", July 2015, 28 p., available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/565890/EPRS_IDA%282015%29565890_EN.pdf.

- *OECD*

Organisation for economic co-operation and development (OECD), "Policy issues in data protection and privacy. Concepts and perspectives", *OECD Informatics Studies*, 1976, nr. 10, OECD, Paris, 324 p.

Organisation for economic co-operation and development (OECD), "Transborder Data Flows and the Protection of Privacy", *Information Computer Communications Policy*, 1979, nr. 1, OECD, Paris, 335 p.

Organisation for economic co-operation and development (OECD), Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, Paris, 32 p.

Organisation for economic co-operation and development (OECD), *Privacy and data protection: issues and challenges*, OECD, Paris, 1994, 71 p.

Organisation for economic co-operation and development (OECD), *The Economic and Social Role of Internet Intermediaries*, 2010, Paris, OECD Publishing, 49 p., available at http://www.oecd.org/internet/ieconomy/44949023.pdf.

Organisation for economic co-operation and development (OECD), *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, 2011, Paris, OECD Publishing, 183 p., available at http://www.oecd.org/sti/ieconomy/49338380.pdf.

Organisation for economic co-operation and development (OECD), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", *OECD Digital Economy Papers* 2011, No. 176, Paris, OECD Publishing, 176 p. available at http://dx.doi.org/10.1787/5kgf09z90c31-en.

Organisation for economic co-operation and development (OECD), "The App Economy", *OECD Digital Economy Papers* 2013, No. 230, Paris, OECD Publishing, 57 p., available at http://dx.doi.org/10.1787/5k3ttftlv95k-en.

Organisation for economic co-operation and development (OECD), *Supplementary explanatory memorandum to the revised recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, 2013, Paris, p. 19-27, available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

Organisation for economic co-operation and development (OECD), "Exploring data-driven innovation as a new source of growth: Mapping the policy issues raised by "big data"", in OECD, *Supporting Investment in Knowledge Capital, Growth and Innovation*, 2013, Paris, OECD Publishing, 306 p.

- *Hesse*

Hessischer Landtag, *Plenarprotokolle der 77. Sitzung*, 8 Juli 1970, 6. Wahlperiode, Stenographischer Bericht nr. 77, 74 p.

Hessischer Landtag, *Plenarprotokolle der 80. Sitzung*, 30 September 1970, 6. Wahlperiode, Stenographischer Bericht nr. 80, 115 p.

Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Ersten Tätighkeitsbericht*, 29 March 1972, 7. Wahlperiode, Drucksache 7/1495, 40 p.

Hessischer Landtag, *Vorlage des Datenshutzbeauftragten betreffend den Vierten Tätighkeitsbericht*, 26 March 1975, 8. Wahlperiode, Drucksache 8/438, 44 p.

- *Belgium*

Deprest, J. and Robben, F., *eGovernment: the approach of the Belgian federal administration*, 2003, 57 p.

- *France*

Commission Nationale de l'Informatique et des Libertés (CNIL), *Premier rapport au Président de la République et au Parlement 1978-1980*, La Documentation Française, Paris, 1980, 219 p.

- *United Kingdom*

Home Office (Great Brittain), *Report of the Committee on Privacy*, Cmnd. 5012, HMSO, London, 1972, 349 p. (the "Younger report")

Home Office (Great Brittain), *Computers and Privacy*, Cmnd. 653, Her Majesty's Stationary Office (HMSO), London, 1975, 13 p.; reproduced by Home Office (Great Brittain), *Report of the Committee on Data Protection*, Cmnd. 7341, HMSO, London, 1978, 460 p.

Home Office (Great Brittain), *Report of the Committee on Data Protection*, Cmnd. 7341, HMSO, London, 1978, 460 p. (the "Lindop report")

Home Office (Great Brittain), Data Protection: the Government's proposal for Legislation, Cmnd. 8539, HMSO, London, 1982, 23 p.

House of Lords, European Union Committee, "EU Data Protection Law: A 'right to be forgotten'?", *HL Paper* 40, London, The Stationary Office Limited, 30 July 2014, 24 p.

- *United States*

Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, FTC Report, March 2012, 112 p.

U.S. Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes", Office of Oversight and Investigations – Majority Staff, Staff Report for Chairman Rockefeller, 2013, 42 p.

OTHER REPORTS

Alhadeff, J. and Van Alsenoy, B. (eds.), "Requirements: Privacy, governance and contractual options", *Trusted Architecture for Securely Shared Services* (TAS^3), Deliverable 6.1, v2.0, 2009, 80 p., available at http://vds1628.sivit.org/tas3/content/deliverables/TAS3_D6p1_v2_TRequirements:_Privacy,_governance_and_contractual_options.pdf.

Alhadeff, J. and Van Alsenoy, B. (eds.), "D6.2 Contractual framework", *Trusted Architecture for Securely Shared Services* (TAS^3), v2.0, 2009, 123 p., available at http://vds1628.sivit.org/tas3/content/deliverables/TAS3_D6p2_v2_TContractual_Framework.pdf.

Alhadeff, J. and Van Alsenoy, B. (eds.), "Legal and Policy handbook for TAS^3 implementations", *Trusted Architecture for Securely Shared Services* (TAS^3), Deliverable 6.1-6.2, v1.0, 2012, 331 p., available at http://homes.esat.kuleuven.ac.be/~decockd/tas3/final.deliverables/pm48/TAS3-D06p1-2_Legal_and_Policy_Handbook_final_versionforthereviewers.pdf.

Ausloos, J., Lievens, E., Kindt, E. and Dumortier, J., "Guidelines for privacy-friendly default settings", *SPION*, Deliverable D6.4, 2012, 37 p., available at www.spion.me.

Badger, L. Grance, T., Patt-Corner, R. and Voas, J., *Cloud Computing Synopsis and Recommendations*, NIST Special Publication 800-146, National Institute of Standards and Technology (NIST), May 2012, 81 p.

Bigo, D., a.o., "Fighting cyber crime and protecting privacy in the cloud", Study for the European Parliament, Committee on Civil Liberties, Justice and Home Affairs, PE 462.509, 2012, 63 p.

Bruegger, B., "Reference Architecture", FutureID deliverable D21.4, v1.1. 2014, 108 p., available at http://futureid.eu/data/deliverables/year1/Public/FutureID_D21.04_WP21_v1.1_Reference%20Architecture.pdf.

Buitelaar, J.C., Meints, M. and Van Alsenoy, B. (eds.), "Conceptual Framework for Identity Management in eGovernment", *FIDIS*, Deliverable D16.1, 2008, 143 p, available at http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_04_16_D16.1_Framework_IDM_in_eGov_Final_2__1_.pdf.

Buitelaar, J.C., Meints, M. and Kindt, E., "Towards requirements for privacy-friendly identity management in eGovernment", *FIDIS*, Deliverable D16.3, 2009, 88 p, available at http://fidis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_06_14_Fidis_D16.3_Reqs_PF_eGov_v1.2_final.pdf.

Capgemini, IDC, Sogeti, and Politecnico di Milano, "Future-proofing eGovernment for a Digital Single Market", Final Insight Report, June 2015, Study prepared for the European Commission DG Communications Networks, Content and Technology, 2015,37 p.

Catteddu, D. and Hogben G., (eds.), *Cloud computing - Benefits, risks and recommendations for information security*, ENISA, 2009, 125 p.

Deadman S., (ed.), "Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation", *Liberty Alliance Project*, February 23, 2005, 34 p.

Decker, M. and Hogben, G., *Appstore security: 5 lines of defence against malware*, ENISA, 2011, 20 p.,

European Network and Information Security Agency (ENISA), "Online as soon as it happens", *ENISA*, February 2010, 49 p.

Farkas, L. and O'Farrell, L., "Reversing the burden of proof: Practical dilemma's at the European and national level", European Commission, Directorate-General for Justice and Consumers, 2015, 100 p.

Graux, H. and Majava, J., "eID Interoperability for PEGS. Analysis and Assessment of similarities and differences – Impact on eID interoperability", *IDABC*, 2007, 210 p.

Graux, H., "Initial Data Protection Report", *STORK 2.0*, Deliverable D3.7, 20 November 2012, 20 p., available at https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=9:d37-initial-data-protection-report&Itemid=175.

Graux, H., "Consolidated Data Protection Report", *STORK 2.0*, Deliverable D3.8, 9 October 2015, 39 p., available at https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=74:d38-consolidated-data-protection-report&Itemid=175

Hon, K, Kosta, E., Millard, C. and Stefanatou, D., "White paper on the proposed data protection regulation", *Cloud Accountability Project*, 28 February 2014, 49 p., available at http://www.a4cloud.eu/sites/default/files/D25.1%20White%20paper%20on%20new%20Data%20Protection%20Framework.pdf

Huysmans, X. and Van Alsenoy, B. (eds.), D1.3 Conceptual Framework – Annex I. Glossary of Terms, IDEM, v1.07, 2007, 36 p.

International Chamber of Commerce (ICC), ICC Task Force on Privacy and the Protection of Personal Data, "Summary of the Workshop on the Distinction between Data Controllers and Data Processors", Paris, Thursday, 25 October, 2007, 6 p.

Irion, K and Luchetta, G., "Online Personal Data Processing and EU Data Protection Reform – Report of the CEPS Digital Forum, Centre for European Policy Studies (CEPS), April 2013, 97 p.

ISO/IEC Information technology -- Security techniques -- Entity authentication assurance framework, ISO/IEC 29115:2013(E), 1 April 2013, 36 p.

International Telecommunication Union (ITU), Telecommunication Standardization Sector Focus Group on Identity Management, Report on Identity Management Framework for Global Interoperability, 30 p., published online https://www.itu.int/ITU-T/studygroups/com17/fgidm.

International Telecommunication Union (ITU), Entity authentication assurance framework, Recommendation ITU-T X.1254, September 2012, 44 p., available at https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11608.

International Telecommunication Union (ITU), "Security Compendium. Part 2 – Approved ITU-T Security Definitions", ITU-T SG 17, 13 May 2005, 52 p., available at http://www.itu.int/ITU-T/studygroups/com17/def005.doc.

Konarski, X., Karwala, D., Schulte-Nölke, H. and Charlton, C., "Reforming the Data Protection Package", Study commissioned by the European Parliament, Directorate-

General for Internal Policies, Policy Department A: Economic and Scientific Policy, IP/A/IMCO/ST/2012-02, PE 492.431, September 2012, 92 p., accessible at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492431/IPOL-IMCO_ET%282012%29492431_EN.pdf.

Korff, D., "EC Study on Implementation of Data Protection Directive 95/46/EC", Study Contract ETD/2001/B5-3001/A/49, 2002, 253 p., accessible at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667

Kuczerawy, A., "Legal and ethical analysis", *Exploiting Social Networks for Building the Future Internet of Services* (SocIoS), Deliverable D3.5, v0.3, 2012, 45 p.

Larouche, P., Peitz, M. and Purtova, N., "Consumer privacy in network industries – A CERRE Policy Report", *Centre on Regulation in Europe*, 25 January 2016, 74 p., available at http://cerre.eu/sites/cerre/files/160125_CERRE_Privacy_Final.pdf

Le Borgne-Bachschmidt, F. et al., "User-Created-Content: Supporting a participative Information Society", Study for the European Commission, SMART 2007/2008, 2008, 302 p., available at http://www.ivir.nl/publicaties/download/233.

Modinis project, Common Terminological Framework for Interoperable Electronic Identity Management, Consultation Paper, prepared for the eGovernment Unit of DG Information Society and Media of the European Commission, v2.01, 23 November 2005, 18 p., accessible at: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf

Olsen, T. and Mahler, T., "Privacy – Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *Legal IST* project, Deliverable D11, 4 November 2005, 144 p.

Robinson, N., Graux, H., Botterman, M. and Valeri, L., "Review of the European Data Protection Directive", *RAND Europe*, 2009, 100 p.

Ruggie, J., "Protect, Respect and Remedy - A Framework for Business and Human Rights", Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises, *innovations* (a United Nations publication), 2008, p. 189-212.

Ruggie, J., "Clarifying the Concepts of "Sphere of influence" and "Complicity"", Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises, A/HRC/8/16, 15 May 2008, 22 p., available at http://198.170.85.29/Ruggie-companion-report-15-May-2008.pdf.

von Bar, C. a.o. (eds.) "Principles, Definitions and Model Rules of European Private Law - Draft Common Frame of Reference (DCFR)", Study Group on a European Civil Code and the Research Group on EC Private Law, 2009, 4795 p., accessible at http://ec.europa.eu/justice/contract/files/european-private-law_en.pdf.

Van Alsenoy, B. "E-government Solutions: Trends and Developments in Belgian e-Government", in M. Meints and H. Zwingelberg (eds.), *Identity Management Systems - recent developments*, *FIDIS*, Deliverable D3.17, 2009, p. 39-49, accessible at http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf.

Van Alsenoy, B., Vandezande, N., Janssen, K, a.o., "Legal Provisions for Deploying INDI services", Global Identity Networking for Individuals (GINI), Deliverable D3.1, 2011, 83 p.

Van Alsenoy, B., Verdoodt, V., Heyman, R., Ausloos, J., Wauters; E. and Acar, G. "From social media service to advertising network - A critical analysis of Facebook's Revised Policies and Terms", v1.3, 25 August 2015, 109 p.

Van Eecke, P., Truyens, M., et al. (eds.), "The future of online privacy and data protection, EU study on the Legal analysis of a Single Market for the Information Society – New rules for a new age?", *DLA Piper*, November 2009, 69 p.

Zwenne, G.-J., Duthler, A-W., Groothuis, M., a.o., "Eerste fase evaluatie Wet bescherming persoonsgegevens - Literatuuronderzoek en knelpuntenanalyse", Ministerie van Justitie (NL), 2007, 211 p.

X., "The Advisory Council to Google on the Right to be Forgotten", 6 February 2015, 44 p., available at https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view.

7 POLICY DOCUMENTS

EUROPEAN COMMISSION

Commission of the European Communities, "Community Policy on Data Processing", Communication of the Commission to the Council, SEC(73) 4300 final, 21 November 1973, 34 p.

European Commission, "Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC)", COM (2003) 265 final, 15 May 2003, 27p.

European Commission, First Report on the Application of Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on the Directive on Electronic Commerce, COM(2003) 702 final, Brussels, 21 November 2003, 25 p.

European Commission, i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, SEC(2006) 511, 24 April 2006, 12 p., available at

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0173&from=EN

European Commission, A Roadmap for a pan-European eIDM Framework by 2010, 2006, v1.0, 20 p., available at http://ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC), 2010, 17 p., available at: http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf

European Commission, Commission Staff Working Document Online services, including e-commerce, in the Single Market, Brussels, 11 January 2012, SEC(2011) 1641 final, 141 p.

European Commission, Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive, 7 March 2007, COM (2007)87 final, 11 p., accessible at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0087&from=EN

European Commission, "Summary of Replies to the Public Consultation on the Commission's Communication on comprehensive approach on personal data protection in the European Union", 4 November 2010, Annex 4, 22 p.

European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better governance of the Single Market through greater administrative cooperation: A strategy for expanding and developing the Internal Market Information System ('IMI')", 21 February 2011, COM(2011) 75 final, 18 p.

European Commission, "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, COM(2012) 9 final, 25 January 2012, 13 p.

European Commission, "Unleashing the Potential of Cloud Computing in Europe", Communication of the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 529 final, 27 September 2012, 16 p.

STAKEHOLDER RESPONSES

Association of Consumer Credit Information Suppliers (ACCIS), Position paper on proposed Data Protection Regulation, April 2012, 21 p., available at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/accis_en.pdf.

Bird & Bird, "Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", 2009, 4 p., available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/bird_bird_en.pdf.

BEUC, "A Comprehensive Approach on Personal Data Protection in the European Union – European Commission's Communication", 24 January 2011, 18 p., available at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf.

Business Europe, "Commission Proposal on a General Data Protection Regulation", Position Paper, 17 October 2012, 18 p., available at https://www.businesseurope.eu/sites/buseur/files/media/imported/2012-01161-E.pdf

European Banking Federation, "EBF Position on the European Commission's Proposal for a Regulation on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 22 May 2015, 5 p., available at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/ebf_en.pdf

European Privacy Officers Forum (EPOF), "Comments on the Review of European Data Protection Framework", 2009, 12 p., available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/european_privacy_officers_forum_en.pdf

Information Commissioner's Office (ICO), "The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data", 7 p., available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf.

Information Commissioner's Office (ICO), "The Information Commissioner's (United Kingdom) response to A comprehensive approach on personal data protection in the European Union", 14 January 2011, 15 p., accessible at http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf

International Pharmaceutical Privacy Consortium, "Comments in Response to the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", 2009, 10 p., available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/international_pharmaceutical_privacy_consortium_en.pdf

International Chamber of Commerce (ICC), ICC Commission on E-business, IT and Telecoms, "ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data", December 2009, 10 p., available at http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/international_chamber_of_commerce_icc_en.pdf.

INDUSTRY WHITE PAPERS

Microsoft, "Protecting Data and Privacy in the Cloud", *Reactive Security Communications*, 2014, 16 p., available at http://download.microsoft.com/download/2/0/A/20A1529E-65CB-4266-8651-1B57B0E42DAA/Protecting-Data-and-Privacy-in-the-Cloud.pdf

Microsoft, "Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance", April 2015, p. 14, available at https://www.microsoft.com/en-us/Openness/TrustedCloud.

Amazon Web Services, "Whitepaper on EU Data Protection", October 2015, 16 p., available at http://d0.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf.