Position on the Regulation 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)

Table of Contents

EDRi welcomes the European Commission's proposal for a new data protection Regulation. Europe needs a comprehensive reform in order to ensure the protection of its citizens' personal data and privacy, while enhancing legal certainty and competitiveness in a digital single market. We are pleased to see that the proposal highlights the importance of key principles. This is a first, positive step in a long legislative process that in the end will hopefully secure greater respect for and awareness of the fundamental right to data protection and to privacy for European citizens. However, EDRi has a number of general issues with the draft, important concerns on specific points, comments and suggestions on specific issues and textual matters.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Definitions (Article 4 - Regulation)

Introduction

Article 4 of the draft Regulation contains 19 definitions. EDRi welcomes the new definitions listed in section 4(9) to section 4(19). At the same time EDRi believes that a number of definitions and corresponding recitals, including the definitions that already existed under Directive 95/46/EC need improvement and/or clarification.

The definition of data subject and personal data

Section 4(1) defines the concept of a data subject. By declaring all data relating to a data subject 'personal data', the concept of what constitutes a data subject becomes paramount. The definition in the draft is very similar to the current definition in section 2(a) of Directive 95/46/EC. In addition to the current definition, the draft clearly states that a person must be considered identifiable when either the data controller or another natural or legal person can identify the person. EDRi welcomes this explanation of what defines personal data. The words 'or another natural or legal person' ensure the absolute concept of identifiability, allowing for protection of personal data whether the data is being processed by the data controller or another person.

In order to ensure data are indeed adequately protected when processed, the phrase 'means likely to be used' must be interpreted broadly in order to provide sufficient protection to data subjects. Both data controllers and third parties can deploy numerous methods identify a data subject. Moreover, the development of such measures cannot be predicted and so a precautionary principle is essential. A broad interpretation of 'likely means' is therefore necessary in order to assure the protection of these data throughout processing. The AOL release of “anonymous” search results should be used as a reference point in policy-making in this area.[1]

What constitutes identifiable?

EDRi advocates a clear understanding of the term 'identifiable'. Data are often presumed non-identifiable, or anonymous while it in fact still traces back to an individual. Personal data should not be regarded anonymous if the data can still be de-anonymized. 'Masking out' or depersonalisation of personal data are valuable security measures, but such measures should not be used to determine whether data are personal data or not. Recitals 23 and 24 should reflect this view point more clearly.

Online identifiers

In relation to the concept of personal data, EDRi is of the opinion that recital 24 regarding online identifiers is too weak to provide for effective data protection in an online environment. This is very likely to lead to confusion with regard to the status of online identifiers. As the AOL case mentioned above proves, online identifiers, even the simple logging of IP addresses without cookies being used, create (new) personal data. Online behaviour, as a rule, leaves such traces. These traces can be combined with other data relating to the data subject to create user profiles and – often - to identify people or the possibility of identifying them unless the processor knows that the data does not refer to a person. For example, spam filters recognise particular IP addresses as belonging to certain ISP mail servers, which are obviously not data subjects. Such online identifiers must therefore almost in all cases be considered personal data. This should be

1 http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

clearly reflected in both Recital 24 and the definition of personal data.

Identifiability and singling out

Online identifiers can individualise data subjects without identifying them. When data subjects can be singled out without identification, it is possible to treat people differently based on their online behaviour and associated profile. Data that can individualise should therefore also be protected under the Regulation, not least because the ability to individualise carries a strong likelihood of identifiability, as shown by the AOL example.

Definition: consent

EDRi welcomes the strengthening of the definition of consent. Consent is a key aspect of the proposal. However, some additional changes would enable better protection of users in the online environment. Consent should always require active behaviour, both in online and offline environments. The necessity of a "clear affirmative action" could be clearly stated and not only assumed. If changes are needed to the definition of consent, it should be to reaffirm the burden of proof requirement contained in Article 7(1). The definition of consent reflects the efforts to increase the responsibility of data controllers and processors in order to ensure that they see to obtain meaningful consent. To give and/or receive meaningful consent is ultimately what matters. We believe that the criteria of a "freely given specific, informed and explicit" consent allow users to be in a position to give a meaningful consent.

Definition: personal data breach

The definition of the term 'personal data breach' is based on the breach of a security measure. In other words, unwanted loss, disclosure or alteration of personal data without breach of security measures will not constitute a data breach. The same logic applies if there are no security measures in place. Therefore, the reference to the "breach of security measures" should be removed – the cause of the breach is irrelevant.

Definition: main establishment of the controller

The draft regulation provides a definition of main establishment, which is welcomed by EDRi. This definition can prevent confusion about which party must be considered data controller, especially when a group of undertakings process personal data in different locations both within the EU and in third countries. EDRi agrees that the establishment that exercises real control over the data processing must be considered data controller. The location of the main establishment will also determine which data protection authority will act as lead authority (see article 51(2)). However, recital 28 leaves corporate groups of undertakings a lot of room to choose which one of their establishments will be considered the main establishment. A group of undertakings can for example assign the power to implement data protection rules to a certain establishment by power of attorney. In practice this is likely to lead to 'forum shopping' by companies.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Exceptions

Introduction

EDRi welcomes the fact that the Regulation applies to the processing of personal data in general. However, a number of significant and very broad exceptions provided for in the draft Regulation, if maintained in their current shape, will limit the application of this new legal framework and create new gaps in the protection of personal data. In order to foster uniform application of the new data protection regulation, the scope and number of these exceptions should be limited.

This paper outlines the most controversial exceptions together with their possible impact on the European standard of data protection and the reasons for limiting or removing these provisions.

Material scope: public security exception (Article 2)

According to Article 2 of the draft Regulation, the new data protection regime will not apply to the processing of personal data in the course of any activity concerning national security. The Council of the EU in its revised proposal would like to go even further, by adding the following additional grounds for limiting the applicability of the Regulation: defence, state security (including the economic well-being of the state when the processing operation relates to State security matters).

It seems that these general clauses are broad and flexible enough to contain not only activities that involve data processing by public entities in the context of national security but also data processing performed by private entities if commissioned by the state to carry out activities broadly related to public security, state security, defence or economic well-being of the state. In this context Article 2 might be used to limit the applicability of data subjects' rights not only with regard to public but also private entities. This concern should be addressed. In EDRi's opinion "national security" exception is broad enough to cover various instances of confidential data processing by state authorities and no other general clauses should be added in this article.

Material scope: maintaining separate legal regimes (Article 2)

Article 2 provides that the new Regulation will not apply to data processing: (i) by the European Union institutions, bodies, offices and agencies; (ii) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (iii) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. These exceptions implicate the continuation of separate data protection regimes for different areas. Except for the first exception, which is outside the scope of Union law, there is no convincing reason for maintaining separate legal regimes. All processing falling in any way under Union law should be covered by the Regulation, although in specific contexts, restrictions might be appropriate.

Material scope: personal or household activity (Article 2)

Article 2 provides that the new Regulation will not apply to data processing "by a natural person without any gainful interest in the course of its own exclusively personal or household activity". The same exception is contained in the Data Protection Directive and, therefore, well established in the European data protection jurisprudence. On the basis of this jurisprudence it is clear that the definition of "exclusively personal or household activity" becomes more and more problematic in

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

the world, where access to digital technologies that enable massive data processing is so common. In particular, this challenge is posed by the use of social networking services that enable processing of vast amounts of personal data and making this data accessible for literally unlimited number of users. In these circumstances it seems that maintaining equally broad exception for personal or household activity in the new Regulation will pose an increasing danger for data protection as there will be no legal instrument to defend data protection standards versus natural persons in their online activity.

In the context of the aforementioned challenges, EDRi welcomed a limitation of the exception for personal or household activity, namely providing that it applies only as long as data is not made available outside the immediate circle of such personal or household activity. This limitation was included in the inter-service draft circulated by the European Commission but was removed in the course of further legislative works. In EDRi's opinion this limitation should be re-introduced.

Material scope: relationship with e-Commerce Directive

According to Article 2(3), the new 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". While EDRi welcomes the concept of ensuring that the level of legal protection for intermediaries as provided in the e-Commerce Directive is maintained, in our opinion the relationship between these two legal acts should be further clarified. It is often the case that data protection standards are infringed not only by reckless or intentional behaviour of a given user (sharing personal data of other individuals) but also by the intermediary, who designed the service in the breach of respective standards. There is a variety of scenarios, where liability for the breach of data protection regulations may be shared, which will pose a serious challenge for jurisprudence.

Territorial scope: Interpretative doubts (Article 3)

According to Article 3(1) of the draft Regulation, as far as its territorial scope is concerned, it will apply to the processing of data "in the context of the activities of an establishment of a controller or a processor in the Union". This phrase has been maintained from the current drafting of the Data Protection Directive. It should be noted that, on the basis of existing jurisprudence, that the very concept of data processing "in the context of the activities" posed serious interpretative difficulties in the course of implementing the Data Protection Directive. Therefore Article 29 Working Party and other authorities suggested that this phrase should be clarified. EDRi supports this recommendation in order to avoid potential disputes when data processing, in particular in on-line environment, is carried out "in the context of the activities of an establishment" and when not. EDRi feels that the established rules for the applicable law on for cross border sales of goods (as provided by for example the United Nations Convention on Contracts for the International Sale of Goods) provide a possible template for the rules to establish the territorial scope for the Regulation.

Another potential interpretative challenge may be posed by Article 3(2), which provides that the new Regulation will apply to the processing of personal data if the processing activities are related to the offering of goods or services. In on-line environment vast majority of services is offered "for free" in the sense that service providers have other sources of revenue than users' fees (e.g.

advertisement). Having that in mind it is very likely that the main question to be asked by the judges and Data Protection Authorities while applying Article 3(2) in practice will be whether it only refers to the offering of goods and services in return for a payment or other form of reciprocation. If the current drafting is maintained it will remain open for diverging interpretations to what extent commercial activity with no money flows between the service provider and the user or services delivered not-for-profit are covered by Article 3(2). In this context, EDRi would welcome adding provision stating that the Regulation would apply "irrespective of whether a payment of the data subject is required".

Processing not allowing identification (Article 10)

Article 10 of the draft Regulation refers to the situation when "data processed by a controller do not permit the controller to identify a natural person" and states that in this case "the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation". While EDRi agrees with the legal concept behind this provision, which constitutes a valid application of the principle of data minimisation, we see a serious challenge in determining when "data processed by a controller do not permit the controller to identify a natural person". The same interpretative doubts are posed by recital 23 of the draft Regulation, which provides that the principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

In EDRi's opinion the new Regulation should account for the challenge of achieving true anonymisation of data in the context of all available identification techniques and the prevalence of databases that enable crosschecks and re-identification of seemingly anonymous data. Therefore, in order to avoid interpretative doubts and potential abuses, additional provisions should be added, determining a number of conditions that need to be met for data to be treated as truly anonymised.

Restrictions (Article 21)

Article 21 provides for a number of general clauses such as "public security", "prevention, investigation, detection and prosecution of criminal offences", "the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions", "other public interests" or "monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority", which can be called upon by both each Member State and the European Union in order to restrict the scope of obligations and rights, which stem from general principles relating to personal data processing.

EDRi welcomes the fact that this possibility is limited by the requirement of proving that such a restriction "constitutes a necessary and proportionate measure in a democratic society". Nevertheless we find the catalogue of potential grounds for restricting the scope of rights of data subjects and respective obligations of data controllers extremely broad and unjustified, especially in the context of general exceptions discussed above with regard to Article 2. The catalogue of permissible reasons for restrictions should be shorter. Similarly, the safeguards to be provided in acts restricting these rights should be strengthened, so that when Member States adopt such acts in accordance with their own constitutional requirements, it is ensured that the fundamental rights of data subjects are not unduly restricted.

Processing of personal data and freedom of expression: national exceptions (Article 80)

According to Article 80 each Member State shall provide for exemptions or derogations from the key provisions of the new Regulation (i.e. on the general data protection principles, on the rights of the data subject, on controller and processor, on the transfer of personal data to third countries and international organisations, on the independent supervisory authorities and on cooperation and consistency) for the sake of protecting freedom of expression (e.g. the processing of personal data carried out solely for journalistic purposes, for the purpose of artistic or literary expression). While EDRi welcomes this acknowledgement of the importance of balancing the right to privacy or data protection and the freedom of expression, the scope and possible implications of Article 80 pose serious concerns.

In particular, EDRi is concerned that due to such a wide scope for national restrictions and exemptions significant divergences in data protection regime applied in each of the Member States will be maintained, thus obstructing the main goal behind moving from the Data Protection Directive to the new Regulation.

In order to take account for the wider use of the Internet and its ability to support freedom of expression through citizen journalism, the restriction to (professional) journalistic purposes of this derogation should be removed. Furthermore, we believe that, both for legal and societal reasons, derogations must be "necessary". Such a limitation would help increase the possibility of a harmonised approach across Europe.

Churches and religious associations: exemption from the supervision of national DPAs (Article 85)

Article 85(1) provides that if churches and religious associations or communities apply, at the time of entry into force of the new Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation. According to Article 85(2) such churches and religious associations are also entitled to establish their own, independent authority in accordance with the provisions relating to national Data Protection Authorities. In EDRi's opinion these provisions will create a very serious exemption, thus limiting supervisory and executive powers of national Data Protection Authorities.

While it can be accepted that churches and religious associations apply their own rules with regard to the processing of personal data as long as these rules fulfil the standards determined in the new Regulation, it is difficult to justify why the practical application of these rules should be supervised by another authority. This situation may lead to the development of diverging lines of jurisprudence and different data protection standards applying to the same or very similar situations depending on quite irrelevant circumstances, which is belonging to a given church or religious association. Therefore EDRi recommends that Article 85(2) be deleted and replaced with a provision making it clear that the application of comprehensive data protection rules developed by a church or religious association will be supervised and executed by the national Data Protection Authority. Moreover, any exceptions for churches and religious associations should be limited to personal data about their own members.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Limitations (Articles 6, 8, 9 and 20 of the Regulation)

Introduction

Articles 6, 8, 9 and 20 of the draft Regulation contain a number of important rules regarding the processing of personal data. These articles determine the legal grounds for processing, the grounds for processing data of children, rules for the processing of special categories of data and rules for the profiling of data subjects. These rules, in particular articles 6 and 20, must set significant minimum safeguards as to the lawfulness of both offline and online processing including for the profiling of data subjects. Data subjects as well as data controllers will both benefit from such strong rules, as they keep data processing fair, predictable and transparent and provide certainty and guidance. The online environment in particular needs strong and clear rules to ensure and, increasingly, to restore trust in online services. Trust is an important condition for the growth of the online sector.

EDRi broadly welcomes the fact that these important articles provide at least a similar level of detail as Directive 95/46/EC. However, the number of limitations to the important principles enumerated by these articles maintain existing loopholes and create new gaps in the protection of personal data. This paper outlines these limitations and describes the problems that they cause. In conclusion, we propose amendments to address these flaws.

Article 6(1)(f), legitimate interest as a legal ground for processing

Article 6(1) defines six grounds for processing of personal data. Legitimate interest currently serves as the basis for virtually unrestricted and unregulated forms of data processing. Examples of these forms of such data processing include direct marketing, fraud detection, monitoring of employees and further use of data originally collected for other purposes.

Using the legitimate interest justification for data processing is appealing for data controllers, because this basis does not carry the same obligations as the other legal grounds included in article 6(1)(a) through 6(1)(e). Legitimate interest allows data controllers to process personal data of data subjects for any purpose, provided that the processing serves a 'legitimate interest' and that the interests of the controller are being *balanced* against the interests or fundamental rights and freedoms of the data subject. However, data controllers will naturally give more weight to their own interests than to those of data subjects. It can therefore not be left to the controller to balance its interests with those of data subjects. It is impossible to verify if the 'balance test' in fact took place as few data subjects have yet been able or willing to test reliance on this criterion in court. This gives data controllers the freedom to let their interests prevail over the theoretical interests of data subjects, causing a serious imbalance. In short, the legitimate interest ground is very broad and its proper use is hard to verify. This leads to uncertainty regarding the scope and lawfulness of certain forms of processing. The more thorough safeguards included in the other grounds for processing suggest that this loophole will be used by even more data controllers in the future.

The online environment has seen a number of cases where data processing was extremely hard to understand and assess. Google's merging of data privacy policies across all its services is one of these examples. The investigations lead by the CNIL have not yet resulted in a clear ruling on the lawfulness of these practices, which are extremely hard to grasp for the average user. In the US, the Federal Trade Commission has four large online multinational companies, namely Google, Facebook, Twitter and Myspace under 20 years consent decrees, requiring them to liaise with the FTC in case of changes to the way they handle the personal data of their users. This measure was introduced as a result of unlawful processing in the past. EDRi firmly believes that such incidents

will lead to a decrease of trust in online services, which is why such situations must be prevented in the EU, by avoiding further unrestrained use of the legitimate interest clause. We therefore suggest amending article 6(1)(f) to achieve the following outcomes:

- Specifically exclude direct marketing as a 'legitimate interest'. Article 6(2) in the interservice draft required consent for direct marketing, which provides a better balance between the rights of data subjects and data controllers. It would also bring this Article more in line with the e-privacy directive, which requires consent for direct marketing and consent for online behavioral advertising. It seems illogical to set lower standards for offline direct marketing. It should also be noted that direct marketing techniques changed significantly since the adoption of the 95/46/EC Directive. Today "direct marketing" often refers to complex and intrusive activities performed by data controllers, such as the use of advanced profiling techniques, behavioral advertising and very precise targeting schemes (sometimes leading to price or service differentiation). It is essential to educate users and increase their awareness of how direct marketing may affect their private life. In this context the requirement of obtaining informed consent may play a vital role to the benefit of the data subjects
- Data subjects should be able to object (opt-out) from any form of processing based on legitimate interest. Opting out must be directly effective and free of charge. Objection must be possible at any moment, including the moment of collection of personal data, via the same channel as the data are being collected or the direct marketing is being sent. Recital 38 as well as Article 6(5) must be amended to achieve this and no longer contain a reference to 'specific situations' as a prerequisite for objection based on legitimate interest.
- Clarify the meaning of the 'legitimate interest' provision in the preamble. Recitals should clarify what will be considered legitimate interests, define the notion of data subjects' interests in more details and clarify how these interests should be weighed or verified.
- Clarify that public authorities cannot rely on Article 6(1)(f) as a ground for lawfulness, in line with recital 38. The current drafting is unclear.

Article 6(4): further non-compatible use of personal data

Purpose limitation is one of the pillars of data protection law. By specifying for which specific purpose data are being collected and used, it is possible for data subjects to give their informed consent or object to such use. Directive 95/46/EC established that data could only be processed further, e.g. for other, new purposes, provided that such further use is *compatible* with the original purpose and the data subject is informed about such use. This requirement keeps data processing fair, transparent and predictable.

The Regulation, in article 6(4), leaves this principle behind and states that further use of personal data is permitted, even if such use is *incompatible* with the purpose for which the data had originally been collected. As stated in the previous paragraph, this damages the very basis of data protection and is inconsistent with one of the fundamental principles of data processing as laid down in article 5(b) of the Regulation, which states that data cannot be processed further for incompatible purposes, be that by the controller or a third party.

Legitimizing further non-compatible use of data will inevitably lead to situations where data subjects are confronted with unexpected instances of such of further use. For instance, one can imagine a case when a data subject has provided his or her data in order to conclude a contract and subsequently finds out the data are further used by this company in order to exercise 'public tasks'. Allowing incompatible use is not transparent, not predictable and not fair, as it creates uncertainty for data subjects and too much leeway for controllers to use, re-use, combine and

transfer data to other parties without restrictions or without being bound to the purpose for which the data were originally collected. Especially in a time where the collection of personal data has greatly increased, and where it becomes more and more clear that personal data are becoming a commodity, the processing thereof must adhere to the principle of purpose limitation. EDRi strongly recommends that article 6(4) be deleted and replaced with guidelines setting the boundaries of compatible further use of personal data.

Article 8: processing personal data of children

The extra protection of minors as provided by this article must not implicate the need to collect even more data for the mere purpose of determining the age of a child. Secondly, rules for the processing of personal data of children, including methods to obtain verifiable consent, must apply alike for enterprises of all sizes. Relieving smaller enterprises will lead to a gap in the protection of minors given the fact that company size does not relate to the number of records of data subjects (including minors). Furthermore, the size of a business in the digital environment often has little or no relationship to its financial power – the selling of Instagram – which had only ten employees - at the time for a sum of one billion dollars being an example of this.

Article 9: processing of sensitive data

The protection of sensitive data under the Regulation suffers from the following loopholes:

- Member States remain entitled to prohibit certain processing of sensitive personal data, even with the data subjects' consent (Art. 9(2)(a)). This runs counter to the harmonization intended by the Regulation and will inevitably lead to some processing being allowed in some Member States, while being prohibited in others, which is out of line with the broad consensus on consistency.

- Member States are obliged to provide (undefined) "adequate safeguards" in relation to the processing of sensitive data under employment law (Art. 9(2)(b)), as well as in relation to processing of criminal data. Furthermore they must provide (also undefined) "suitable measures" to safeguard data subjects' legitimate interests in relation to the processing of such data when "necessary for the performance of a task carried out in the public interest" (Art. 9(2)(g)). Here again, the risk is created of a lack of harmonisation which, in turn, will lead to forum shopping and a "race to the bottom" in relation to the elimination of data protection standards and safeguards for the protection of the right to privacy.

- The list of sensitive data under the Directive and the Regulation should be identical; beliefs should include philosophical beliefs; criminal convictions as well as offences must both be treated as sensitive data.

Article 20: measures based on profiling

What is profiling exactly and why is it problematic?

Data controllers can create profiles of data subjects by collecting personal data about them. Such profiles and 'categories' of data subjects are being created in order to 'map' a person and to evaluate as well as analyze and predict (future) behavior. When more data become available, the profile becomes more precise and, consequently, becomes more valuable. The creation of profiles relies on increasingly complex algorithms, dynamically corrected and improved. The ever-increasing generation, capture and matching of personal information as well as information about

objects that relate to individuals, such as cars, mobile phones, IP addresses and RFID chips, obtained in very different contexts, and of widely varying quality, create a new data environment that facilitates the ever-wider use of profiles for commercial as well non-commercial purposes. Profiles can be used for many different purposes, from marketing through the screening of job applicants, to credit-referencing and "-scoring", to law enforcement and the fight against terrorism. Online profiling, based on IP addresses and other online identifiers such as cookies, create profiles of internet users based on which they can be identified or singled out in the online environment. On the basis of their online profile, data subjects can be confronted with special offers, while other content may be withheld or prioritized differently.

Generally speaking, EDRi recognizes three main problems in relation to profiling of data subjects:

– Profiles can get it wrong, particularly when assessing uncommon characteristics. Where a profile is used as the basis for a fully automated decision, there is a risk that this decision is made on the basis of data that statistically apply to this person but that nonetheless give a wrongful impression of this person's behavior, health, preferences or reliability.

– Profiles can be hard or impossible to verify. Profiles are based on complex and dynamic algorithms that evolve constantly and that are hard to explain to data subjects. Often, these algorithms qualify as commercial secrets and will not be easily provided to data subjects. This non-transparency undermines trust in data processing and may lead to loss or trust in especially online services. There is a serious risk of unreliable and (in effect) discriminatory profiles being widely used, in matters of real importance to individuals and groups, without the required checks and balances to counter these defects.

– Profiles are likely to perpetuate and reinforce societal inequality and discrimination against racial, ethnic, religious or other minorities; this risk grows dramatically with the massive, almost explosive growth in data we are witnessing today. Continuous close scrutiny of the outcomes of decisions based on profiles, and of the underlying algorithms, is essential if these effects are to be avoided. Profiling creates an inherent risk of discrimination (e.g. in the context of access to goods and services) or other forms of unfair treatment, in particular increased surveillance if it is performed by public entities either directly or using data collected and processed by private companies.

What are the rules for profiling and what amendments are necessary?

Article 20 contains rules with respect to profiling. It states that every person has the right not to be subjected to measures that produces legal effects if these measures are solely based on automated processing. In order to build profiles of data subjects as described above, personal data is being collected and categorized. Both the collection and categorization can take place on one out of six legal grounds (article 6(1)), including the legitimate interest of the data controller. Sadly, the right not to be subjected to automated decisions is being diluted in article 20(2) through to article 20(4), resulting in too few safeguards against the negative effects of profiling on data subjects' privacy and other rights. EDRi proposes the following changes in order to protect data subjects from unwanted consequences of profiling.

– Article 20(1) should state explicitly that it applies to all kinds of profiling, both online and offline. It is clear that the online environment allows for the creation of profiles of data subjects based on their behavior, through cookies, device fingerprinting or other means of gathering of user data.

– In order to regulate online profiling activities, it is necessary to recognise that online

identifiers are personal data. Contrary to the initial draft and the interservice version, recital 24 currently states that online identifiers do not *necessarily* have to be considered personal data. This creates uncertainty as well as a legal loophole because it means that profiling online can take place based on these so-called identifiers, without the guarantee that the Regulation applies. EDRi therefore proposes the deletion of this recital, replacing it with the recital originally included in the interservice version, which stated that the Regulation will apply to online identifiers because these are associated with individuals and because online identifiers leave traces which can be used to create profiles of the individuals and identify them or single them out.

– Article 20(2)(a) must include the right for data subjects to be provided with meaningful information about the logic used in the profiling as part of the information duty applicable to data controllers, and, if human intervention has been obtained, the right to an explanation of the decision reached after such intervention. Also, data controllers must be accountable to DPAs in case there is a need for a DPA to assess whether profiling was lawful or not. They must therefore document the results of profiling and be able to demonstrate that profiling does not lead to discrimination. This will help make profiling more transparent and prevent discriminatory practices.

– Where Union or Member State law provides for 'suitable measures', as referred to in article 20(2)(b), such measures must specifically contain protection against discrimination as a result of automated decisions (profiling). This requirement also applies to the 'suitable safeguards' that must exist in the case where data subjects give their informed consent to the profiling.

– Use of sensitive personal data: in the private sector, profiling may never be based on or include sensitive personal data. In the public sector, profiling shall only involve use of sensitive personal data when these data are manifestly relevant, necessary and proportionate to the purposes of the legitimate public interest pursued, and even then should never be based solely or predominantly on those special categories of personal data.

– The Commission must adopt delegated acts for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subjects' legitimate interests referred to in paragraph 2 within six months of entry in to force and after consultation of the Data Protection Board on these proposals.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Consent

Introduction

Clarifying and strengthening the obligations for consent is a very important point for EDRi. The failings in the implementation of the existing Directive are well known (see for example the Commission impact assessment[2]). The Eurobarometer 359 survey[3] showed that 70 % of Europeans are concerned about how companies use their data and feel they have only partial if any control; 74% want to be asked to give specific consent before their information are collected and processed.

There are three features of data collection that make the current rules on consent ineffective:

- Technology has evolved rapidly and become so sophisticated that data subjects do not know and/or are not aware that their data are being collected and processed, or when this happened, or what data are being collected and processed, or the amount of data involved (so-called invisible data mining). Nor do they have any knowledge of the extent to which the processing is potentially sensitive, or how it can affect them - or indeed of the purpose for which their data are used.
- The information provided by controllers is typically either obscure and legalistic or hidden in rarely-read privacy notices, which means that data subjects are not taking informed decisions.
- Controllers often find ways to claim that consent was given by users (e.g., through opt-outs, pre-ticked boxes, etc) without users/consumers in reality having given free and informed consent.

Eliminating deceptive practices

The draft Regulation's definition of and conditions for consent reflect efforts to increase the responsibility of data controllers and processors in order to ensure that they seek to obtain meaningful consent. Data controllers must provide evidence of consent according to defined standards. We feel that behavioural economic research should be carried out on how free and informed consent at present really is and to frame the kind of information companies should give and how to design the information.

EDRi believes that consent is a key aspect of the proposal for a Regulation, and that consent should always be the result of an active choice, as referred to in Recital 25, and should not be assumed on the basis of a data subject's perceived behaviour. Not changing default settings should certainly not be interpreted as consent to whatever these settings allow.

The definition provided in Article 4(8) should therefore remain unchanged

Nonetheless, Article 6(1) provides a list of six criteria for lawful processing, and consent is only one of these. EDRi thinks that among these there is an important loophole that can be used by data processors to justify any processing of personal data, namely the concept of "legitimate interest" in the "balance" provision contained in Article 6(1)(f). This provision can in practice offer controllers a way to avoid many processing restrictions altogether, since current experience suggests that few data subjects will be able or willing to test reliance on this criterion in court. Moreover, the

2 http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

3 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

broadness of the term “legitimate interest” creates legal uncertainty, both for data subjects and business. Furthermore this uncertainty will most probably lead to divergences in practice between different member states and therefore a failure to achieve the goal of harmonisation. Policy should be developed based on the principle that data processors are intrinsically incapable to balance their interests with that of data subjects' right to privacy.

If a data controller wishes to use “legitimate interest” as a basis for processing, this must be separately and explicitly flagged to the data subject and the data processor should publish its grounds for believing that its interests override those of the data subject.

If changes are needed to the definition (Article 4(8)), it should be to echo the burden of proof requirement contained in Article 7(1). It is indeed crucial that consent be demonstrable and, of course, that the burden of proof remain with controllers; data subjects should not be required to prove that consent was not given.

In EDRi’s view, it is not a good idea to try to define means of expressing consent in legislation: there are more possibilities than just opt-in and opt-out. Instead, the relevant means of expression need to be adapted to the circumstances. This approach supports our contention that the burden of proof should rest on the controller. In the interest of data minimisation, it would also be useful to expressly clarify in the text of the Regulation that collecting data that are not necessary for or relevant to the purpose in question cannot be justified on the basis that the controller has a “legitimate interest” in collecting the data, e.g., for proof of consent purposes.

Significant imbalance

Concerning the term “significant imbalance” in Article 7(4), EDRi believes that the examples given in the Recital are too narrow. The phrase should cover all situations where there is a serious difference in power. A similar non-exhaustive list to the one in the Unfair Contract Terms Directive should be added in Recital 34 illustrating what “significant imbalance” means, including, for example, situations of *de iure* or *de facto* monopolies and oligopolies which, in practice, offer users/consumers no real opportunity to choose a privacy-respecting service provider. Similarly, where a data subject has spent years developing his/her persona in an online game or on a social network, a “take it or leave it” change of terms of service by the operator would clearly leave the user in a very weak position *vis à vis* the provider.

On the possibility of having a contextual approach to consent, EDRi believes that what matters is that the given consent is meaningful. In our opinion, the criteria of a “freely given specific, informed and explicit” consent allow users to be in a position to give meaningful consent. To undermine these requirements would be to undermine the Regulation itself – any flexibility offered to business should not be allowed to undermine the core elements of the exercise of the fundamental right to privacy.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Interaction with the data subject

Introduction

EDRi broadly welcomes the provisions in the Regulation, which strengthen and clarify the rights of the data subject through measures aiming for greater accountability and responsibility of the controller (eg - to inform data subjects of breaches, to ensure greater transparency of data processing and greater access to remedies), as well as rights such as data portability. Additionally, EDRi supports the clarification and better implementation of current rights including the right to erasure (through the right to be forgotten).

There are however some provisions that could be clarified and strengthened to avoid any potential restrictions on the right of the user to exercise their right to data protection.

Processing of Data of Minors (Article 8)

EDRi sees the need to clarify specific rules for the processing of data of children, and agrees that processing of data for data subjects under the age of 13 the data subject should require parental consent. Considering that data can be processed in other situations outside of the scope of "the offering of information society services", as Article 8(1) indicates, we suggest broadening the scope to include all services.

Transparency and Modality, Information and Access to Data (Articles 11-14)

EDRi considers the addition of greater transparency and accountability mechanisms to be a significant improvement compared with those outlined in Article 10 and 11 of the 95/46/EC Directive. Particularly given the nebulous nature of many Terms of Service and Privacy Policies, we welcome the requirement in Article 11(2) to ensure processing of personal data is communicated to the data subject in intelligible form, using clear and plain language. However, in communicating the rectification or erasure of data, Article 13 requires clarification as to what "a disproportionate effort" may entail for the controller as a reason for not being able to do so.

Article 14, which provides a list of mandatory information to be provided to the data subject is also a welcome addition. However Article 14(1)(h) should further specify that "additional information" should include any processing operations that would have particular impacts on, or consequences for, the data subject, for example for measures based on profiling (Article 20) or in cases where the privacy impact assessment (Article 33) reveals significant risk.

Rectification and Erasure, Right to Object and Profiling (Articles 15-19)

Right to be forgotten (Article 17)

Article 17 builds primarily on rights that currently exist under the 95/46/EC Directive. However, as the article stands, it is unclear how this could be implemented in practice, particularly in an online environment.

To ensure greater clarity, we suggest refining the text in order to ensure that controllers are responsible for "the right to be forgotten" in relation to data over which they have control. Where controllers have lost control of data in ways which contravene this Regulation, this should be subject to appropriate sanctions. However, attempting to make online services, in particular, liable for the availability of content over which they have no control will lead to measures (blocking,

filtering, de-indexing, etc) that contravene the freedom of communication and could even lead to the introduction of technologies which would undermine their privacy (measures such as those prohibited by the Scarlet/Sabam ruling of the European Court of Justice (Case C70/10) , for example).

For these same reasons, we suggest broadening the scope of article 80 to include "all media" to ensure the protection of the right to free expression. Finally, the data subject should not have to invoke the right to deletion in Article 17.1(c) and (d), as this right is already articulated in Article 5(e).

Right to Data Portability (Article 18)

EDRi welcomes the inclusion of this new right, but the scope must be broadened to include not only data collected on the basis of consent or a contract to data collected through other means. Where Article 18(1) refers to an "electronic and structured format which is commonly used", we suggest refining the term "commonly used" by specifying that this includes interoperable and open source formats.

Right to Object (Article 19)

EDRi supports the strengthening of the right to object, particularly as the burden of proof to demonstrate "legitimate interest" falls on the processor and not the data subject.

Article 19(2) should expand "intelligible manner" using the language in Article 11(2).[4]

Remedies, Liabilities and Sanctions (Articles 73-77)

EDRi views the establishment of comprehensive and streamlined remedies for data subjects as an essential element of the Regulation. However there are several aspects in Chapter VIII which require further specification, particularly in regard to the application of sanctions.

Collective & Individual Actions

Article 73 states that a data subject or any appropriate body (organisation or association) can launch a complaint to a supervisory authority. What is lacking however is the inclusion of collective action, as this type of redress mechanism could empower data subjects and increase the effectiveness of compliance with data protection law. By enabling such collective action, individuals would be more likely to report smaller scale but widespread violations, as they would be much less deterred by administrative burdens, potential costs and other such risks.

Competence of Courts and DPAs

EDRi welcomes the attempt to create a flexible system of redress for data subjects, enabling them to file actions in the country they reside. However, this approach could result in an unintentional complication of redress, where supervisory authorities, the court and the controller could be in different Member States. While Article 76(3) and (4) attempt to address this potential situation, EDRi suggests further clarification, particularly with a view to ensuring greater information sharing on the level of national courts.

4 Where any communication relating to the processing of personal data should be communicated in "an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child"

Similarly with regard to data protection authorities, Article 76 should include clear articulation the role of the Board in a case of conflict between two authorities, as EDRi can envision cases where individual DPAs may take opposing views in a single court case (Article 76(2)), which would likely not result in the strengthening of rights for the data subject, in addition to potentially deterring cooperation and trust between DPAs.

Court Proceedings

On the exception of bringing proceedings to court of the data subject's place of residence not applying if the controller is a public authority (75(2)), EDRi strongly suggests ensuring that this exception does not apply to public authorities of third countries, as this would effectively deprive data subjects of adequate redress mechanisms.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Tasks and Obligations

Conditions for Consent (Article 7)

EDRi welcomes the fact that Article 7(1) places the burden of proof on the controller, as well as introducing safeguards to verify the validity of the consent in the cases of significant imbalance between the position of the data subject and the controller.

General Obligations

As a general remark, the exceptions provided to SMEs regarding compliance with the Regulation are acceptable, provided that citizens have the same protections regardless of the size of the enterprise or body that is processing their personal data. The essence of the right may not be diluted and, therefore, it should be made explicitly clear that such exceptions apply only to Chapter IV and not the Regulation as a whole.

Responsibility of the Controller (Article 22 & 28)

EDRi welcomes that Article 22 (paragraphs 1 and 3) obliges the controller to ensure and demonstrate compliance, and sees this as an effective way or ensuring accountability on the part of the controller. To add further clarity to Article 22(2), we suggest adding a reference to Article 11 on transparent information and communication. Furthermore, it should be made clear in the Regulation that the principle of accountability shall not be limited to the elements listed in Article 22(2).

In line with the provisions in Article 11, Article 22(3) should be strengthened to include that such verifications ensuring the effectiveness of measures in (1) and (2) must be done transparently and made publicly available. Such "transparency reports" should include the information referred to in Article 22(1) and (2). EDRi also questions the ability of verifications to be truly independent if they are carried out by internal auditors.

In order to maximise efficiency and effectiveness, industry sectors should cooperate with supervisory authorities to harmonise such compliance documentation, creating economies of scale for business and predictability and transparency for citizens and supervisory authorities.

Data protection by design and by default (Article 23)

EDRi welcomes the inclusion of a separate Article on data protection by design and by default, however, the current drafting of this article lacks a clear definition and practical applications. In order to operationalise these obligations, we strongly suggest the following changes:

Firstly, include a clear definition of data protection by design in recital 61. This could say for example, "Data protection by design is the process by which data protection and privacy are integrated in the development of products and services through both technical and organisational measures." This definition should be further specified by adding *1(a) Technical measures*, which refer to the physical design of products, such as hardware and software; and *1(b) Organisational measures*, which include external and internal policies, current best practices.

Similarly, the definition of privacy by default (paragraph (2)) also needs to be more specific and include references to both the technical and organisational aspects. We therefore suggest the same delineation of 23(*2*)(a) *Technical measures*, referring to data settings in hardware and software by companies; and *2(b) Organisational measures*, referring to privacy protections

available to the data subject. In this case, the most privacy protective option should be the basis if it is enough to achieve the specific and limited purposes of the collection of data. This includes, for instance, that controllers do not prohibit data subjects from using pseudonyms on their services unless strictly necessary.

On controllers, joint controllers & processors (Articles 24-29)

EDRi agrees that in situations where a controller defines the processing of personal data jointly with others (Article 24), it should be compulsory that they make arrangements between them.

Data Security

Security of processing (Article 30)

Article 30 states that whenever there are risks inherent in the processing of personal data, both the controller and the processor must first evaluate them and then take appropriate security measures. However, specific rules for how to determine the level of security are needed. To this end, EDRi recommends including a reference to Article 33 in 30(2) when referring to “an evaluation of the risks”.

As the Article currently stands, it is not clear whether the controller or processor, or both equally, have responsibility. The Article should emphasize that the overall responsibility lies on the controller (as specified in Article 22 and 26).

Data Breach Notification (Articles 31-32)

EDRi is pleased that the Regulation includes a provision on mandatory data breach notification to the data subject (Article 32(1)), however the phrase 'likely to adversely affect' seems too vague and should be further specified. Detailed criteria and requirements are needed for establishing what constitutes a “data breach” and what threshold requires notification. If the Commission chooses to specify this in delegated acts (Article 32(5)), they should be adopted at or before the entry into force ofthe Regulation, to avoid a legal void, however temporary this may be.

As the Regulation seeks to establish greater accountability and transparency, we also suggest that notifications to the data subject should extend the current scope of “at least the information and recommendations provided for in points (b) and (c) of Article 31(3)”, to also cover points (a), (d) and (e) of Article 31 (3).

Finally, while expeditious notification of data breaches are needed, a 24-hour time limit (Article 31(1)) might be difficult to realistically implement, and could potentially undermine the effectiveness of these provisions. Considering that this provision will apply to many different types of controllers, from small companies to large enterprises, one time limit may not be appropriate in all cases. We therefore suggest extending this to 72 hours.

Data protection Impact Assessment (DPIA) (Article 33)

Article 33(2)(a) provides a list of processing operations that includes ambiguous phrases such as “significantly affect the individual” 33(2)(a), or “on a large scale” 33(2)(a),(b), that may obscure the scope of the DPIA.

EDRi recommends stating more clearly that the exception for carrying out a DPIA as it is made in

Article 33(5) only applies if an equivalent assessment has been made in the legislative context.

Data Protection Officer (DPO) (Articles 35-37)

EDRi sees the increased specifications and the mandatory designation of a data protection officer as an improvement from the Directive 95/46/EC, and understands that the DPO's ability to perform his/her job (including informing and advising the controller or processor of their obligations, and to internally oversee application and compliance with the Regulation) requires independence, as indicated in Article 36(2). However, it should be made clear that the DPO is not the only person involved in ensuring compliance with the Regulation (think for example, of Article 23 which introduces obligations that data protection compliance throughout the entire DNA of a company, organisation or body).

To ensure greater clarity, we suggest making explicit reference to the rights mentioned in 37(1)(c), including Articles 23 and 22, 30-32, Articles 11-20.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Transfer of Data to Third Countries

Introduction

Transfer of data to third countries is a politically sensitive subject. The Regulation is trying to serve two goals that appear to be in conflict: protecting data and facilitating the flow of data, including to third countries outside the EU that do not provide for adequate protection of personal data.

General principle (Article 40)

EDRi is concerned with a significant shift in the data protection framework from a general prohibition of transferring data to third countries (notwithstanding derogations) as contained in the Directive to the principle that transfers can only take place if enumerated conditions are met, which has been formulated in the draft Regulation. As a result, more legal grounds permitting the transfer of data to outside the European Union would exist under the Regulation than exist under the Directive. EDRi would welcome a reverse trend and reintroduction of the principle that international transfers of data are, in principle, prohibited, with this prohibition being lifted when essential criteria are respected.
The draft Regulation attempts to clarify the grounds for the responsibility of data controllers and data processors as well as the legal basis allowing international transfers of data including onward transfers. The main problem, however, is that essential safeguards to protect personal data in this context are not sufficiently specific. This creates a serious risk of their misinterpretation, circumvention or other abuses.

Adequacy rule

The adequacy rule is a delicate issue. While EDRi agrees that adequacy does not mean having the exact same rules but rather following the same (adequately enforced) principles, it seems that the Commission's proposal does not take into account the stage of practical implementation of the Regulation. The authority of the European Commission to issue adequacy decisions should be revised thoroughly. In our opinion, the possibility of issuing an adequacy decision should be limited to situations in which the unilateral decision made by the Commission will not be able to affect the level of data protection as guaranteed in the draft Regulation.

The adequacy rule has become bureaucratic and the examination procedure seems to be about looking only at the legislation and not at the way it is implemented – either at the time of approval or on an ongoing basis. Ongoing review must become part of the adequacy procedure. The wording of this provision should be more detailed and rigorous. In many cases, these issues are so important and so closely associated with the protection of fundamental rights that they cannot be regulated solely by a judgement made by the European Commission. The problem is that the Commission is both judge and jury. It would be valuable, also for the credibility of the process, to include additional checks and balances, such as review or appeal possibilities being given to the Data Protection Board and/or national Data Protection Authorities. Giving at least the right to veto on the adequacy decision to the Data Protection Board would eliminate the criticism that there is no counter-balance to the Commission's decisions. Another issue that calls for a more detailed approach is the examination procedure. Experience shows that the formal "examination procedure" implemented by the European Parliament is not, on its own, an adequate safeguard.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Transfers by way of appropriate safeguards

Experience shows that standard clauses do not provide sufficient protection of personal data. Adequate safeguards are necessary; article 42 needs to be more specific and prescriptive. An approach requiring a prior approval from Data Protection Authorities (such as the one foreseen in Article 42(5)) would therefore be preferred for all transfers based on contractual clauses and not only for transfers that take place without a legally binding instrument in place.

Existing safeguards

The Regulation leaves existing adequacy decisions as well as the Safe Harbor framework intact. This is a missed opportunity to reform existing agreements, most particularly the Safe Harbor framework, which has been an unequivocal failure, offering little or no meaningful protection of European data subjects' data.

Standard protection clauses are not sufficient, and more adequate safeguards are necessary.

Binding corporate rules

Binding corporate rules (BCRs) open the way for private arrangements for the protection of exported data and made-to-measure solutions for groups of undertakings. Rules adopted by means of BCRs are not clear to data subjects and thus raise significant transparency issues. The safeguards provided by BCRs are frequently weak and ultimately promise something that cannot be delivered – control by the data controller over data that they have limited practical control over. EDRi believes that rules on BCRs should be revised and strengthened significantly in order toprevent them from being used as a way to legally circumvent obligations without offering appropriate guarantees.

In addition, Paragraph 43(2)d should be amended to include data minimisation and limited storage periods.

Derogations

Article 44 contains a number of derogations that are too vague. There is a clear risk that the protection against real risks associated with transfer of personal data to third countries will be weakened by these broad derogations. Moreover, it should be expected that data controllers will be tempted to rely on derogations instead of providing for appropriate safeguards before deciding to transfer personal data.

The wording of Article 44(1)(d), for example, should be more specific. “Public interest” is too broad, while recital 87 seems to extend the scope of this derogation even more. The range of grounds that may come under a vague label of public interest is therefore clearly too broad, thus creating legal uncertainty for data subjects.

Article 44(1)(h) is specifically of a great concern because it creates endless possibilities for transfers of personal data to third countries. The meaning of “legitimate interest”, as a legal ground for processing, has proven to be extremely broad, thus undermining the protection of data subjects. The draft Regulation should prevent the transfer of personal data from taking place on this vague basis. This problem could be made even worse by the lack of consistency between Data Protection Authorities while applying this general clause in practice. EDRi therefore proposes the deletion this paragraph.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

If the derogations are not carefully re-drafted, they will also allow for transfers of data from private companies to law enforcement authorities without any, or with inadequate, safeguards, undermining the quality and predictability of the protection of the personal data of European data subjects.

When transfers of data are based on derogations, the legal ground claimed should be subject to prior approval and publicly registered. The Commission's proposed text makes it difficult, if not impossible, to guess how Data Protection Authorities will regulate the proposed derogations.

International cooperation

EDRi is concerned about the international cooperation provided for in Article 45. The example of the Safe Harbour with the United States of America is a cautionary one. The FTC (Federal Trade Commission) appears to see its role as a purely bureaucratic one, only acting ex post and in cases of the largest of the breaches of the agreement. The agreement seems more symbolic than practical, doing little or nothing to protect the data subjects in the vast majority of cases. Therefore EDRi would like to express its conviction that the Safe Harbor agreement is wholly inadequate for the protection of the fundamental rights of European data subjects. The entire current EU approach to international data transfers undertaken outside the scope of adequacy findings needs to be carefully redesigned.

Disclosure to third countries by virtue of extra-territorial laws, regulations and other legislative instruments

The draft Regulation in its current version does not address the challenge of data transfers to third countries by virtue of extra-territorial laws, regulations and other legislative instruments, including for the purpose of law enforcement. It should be noted that existing practice in this area is very disquieting. Specific risks are related to the processing of data in cloud computing, when the providers of such services are legally established outside the EU. For example, under the U.S. Foreign Intelligence Surveillance Act of 2008 Act (Article 1881), the U.S. government is entitled to carry out surveillance of European data subjects on the basis of their data being processed by U.S. companies. The draft Regulation does not provide for any specific guarantees in this regard while, at the same time, aims at facilitating the transfer of personal data to third countries.

In the inter-service version of the Regulation (Article 42) it was stated that in the cases of disclosure of data to third countries by virtue of extra-territorial laws, regulations and other legislative instruments prior approval/authorisation of the Data Protection Authorities is required. EDRi regrets that this important safeguard was removed in the course of the latter stages of the inter-service consultation process and urges the European Parliament and Council to re-introduce this measure. Reintroduction of this provision would provide legal certainty for both data subjects and businesses. Having this principle in a recital does not provide a sufficient safeguard for the protection of personal data It is at best inappropriate and, at worst, a breach of the Charter on Fundamental Rights, for this issue not to be clearly and thoroughly addressed by the new Regulation.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Data protection authorities

Introduction

EDRi welcomes the strengthened framework created by the Regulation for independent supervisory authorities i.e. data protection authorities (DPAs). In order to effectively protect personal data, it is important to have a competent, adequately resourced and independent supervisory authorities.

Currently there are excessive disparities between national DPAs and the Regulation must ensure that these differences are eliminated. The legal and technical resources available to DPAs need to be strengthened and equivalent resources need to be given to all DPAs. These resources need to be sufficient to enable DPAs to fulfil their role properly.

While the Regulation does represent a significant step forward, EDRi believes that the Regulation needs additional improvements to ensure that DPAs have sufficient powers and capacity to undertake their role effectively.

Transnational enforcement (Article 56)

Joint investigation is essential when dealing with EU transnational enforcement or with large-scale cases, i.e. involving big companies or when individual DPAs do not have enough resources to adequately deal with certain cases, due to their size or geographic spread. Joint investigation and strong cooperation would create a positive incentive to deal appropriately with large-scale, complex and/or multi-territorial cases. Such a procedure is also needed to ensure that smaller DPAs are not excessively burdened by cases where large companies fall under their jurisdiction. In addition, it would help to prevent the danger of forum shopping when it comes to the enforcement of the new data protection standards, i.e. choosing the place of establishment for the sake of being under the authority of a DPA that does not have the capacity to undertake large-scale investigations on its own.

EDRi therefore welcomes the provisions contained in the Article 56 and recommends that the rights and respective obligations of DPAs in this context be further strengthened. In particular, the wording of Article 56(2) could be improved to the effect that DPAs from all Member States where there are data subjects likely to be affected by processing operations in question, are obliged to participate in joint investigative tasks or joint operations. This is, however, a significant logistical challenge and therefore it may be worth considering whether coordination of such investigative tasks or joint operations when at least half of all Member States are involved could be entrusted to the European Data Protection Board. Finally, it is essential that not only other DPAs are involved in the investigation process but are also consulted when it comes to the final decision being made by the host supervisory authority. An appeal procedure involving the European Data Protection Board should also be introduced if other DPAs involved in the process of investigation question the final decision made by the host supervisory authority.

It is also worth considering the possibility of entrusting both investigatory and decision-making powers to the European Data Protection Board (or equivalent central body) when it comes to dealing with transnational corporations that operate in the whole (or most) of the EU.

Regardless of how this is achieved, the practical effect of Article 56 of the Regulation must be effective enforcement in cases of cross-border or pan-European data processing.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Independence

In accordance with the EU Charter of Fundamental Rights (article 8), the enforcement of data protection laws should be supervised by an independent authority. Independence of DPAs cannot be assured if these authorities are susceptible to political pressure.

The principle of independence of DPAs was nominally imposed by Directive 95/46/EC, which requires DPAs to act fully independently. Section 28(1) of Directive 95/46/EC states that DPAs "shall act with complete independence in exercising the functions entrusted to them".

On 9 March 2010, the ECJ ruled that 'complete independence' means that DPAs may not be subject to state oversight or scrutiny.[5] They must be 'free from any external influence'. The court also stated that any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data must be avoided.[6] Also, the risk that other authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks[7] and thus not consistent with the requirement of independence.

Chapter VI of the draft Regulation states in section 47 that DPAs shall act in complete independence. However, section 48(1) leaves open the possibility for appointment of DPA by the government. In EDRi's opinion this does not ensure full independence as it leaves the door open to political pressure being exerted on DPAs. From the perspective of ensuring full political independence of DPAs, it would be advisable to introduce an explicit clause in the Regulation that would forbid the appointment of members of the supervisory authority by the government. National parliaments should be the only political bodies allowed to appoint DPAs due to their representative nature. There is also one procedure that could be recommended for selecting the candidates for this position (i.e. before the election), namely the system of academic (or scientific) recommendations. In this system the candidates running for the position of a member of supervisory authority are nominated by supervisory or scientific boards of all academic institutions that can confer a degree of the professor of law. This or a similar system would increase the independence of DPAs even more.

The consistency mechanism, introduced in section 2 of chapter VII, gives a lot of power to the Commission in individual cases. According to article 59, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to the consistency mechanism. While EDRi acknowledges that the mere competence to issue an opinion does not limit independence of the DPAs, we are very concerned with the potential implications of article 59(2), which states that: "where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure."

This provision clearly aims at placing the Commission at the same level as the European Data Protection Board, when it comes to the level of legal authority and gives the Commission the power to exert significant pressure on DPAs to comply with its recommendations. In order to limit political influence on DPAs, EDRi recommends that article 59(2) be deleted or rephrased to the effect that opinions issued by the Commission are treated in the same way as any other opinions received by DPAs in the course of their work. The only body that might be endowed with a power to issue semi-

5 ECJ, C- 518/07, Commission v Germany
6 ECJ, C- 518/07, Paragraph 30
7 ECJ, C- 518/07, Paragraph 36

binding opinions in given cases is the European Data Protection Board.

Resources

Financial resources, capacity and skills are necessary to assure the efficiency of the independent supervisory authorities. These resources should include sufficient technical expertise and equipment to ensure that full audits of data processors and controllers are possible. Since data processing is inherently connected to the use to digital and other technologies it is essential that DPAs be endowed with strong and competent technical departments. Moreover, their budget should allow for recruitment of high quality specialists with skills and experience necessary to perform audits in cutting-edge technological companies. Having these prerequisites for effective operation of DPAs in mind, EDRi recommends that an additional clause is added in chapter VI section 1 that will explicitly require that supervisory authority be endowed with a technical department of an adequate size and adequate standard of technical competence.

We suggest adding a provision specifically referring to adequate technical skills of staff the following sentence to the end of Recital 94.

Accountability

EDRi welcomes the right to a judicial remedy against a supervisory authority stated in Article 74. However, it is difficult to imagine the efficiency or even likelihood of the scenario foreseen in Article 74(4), where DPAs are prosecuted by other DPAs.

EDRi would prefer to see the problem approach through some systematic methods, such as reporting or an ombudsman system.

European Data Protection Board – Term of office

Article 69 of the Regulation provides that the European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members and that their term of office shall be five years and be renewable. In EDRi's opinion, this provision should be reconsidered on the basis of what terms of office of DPAs prevail in the EU. It seems very likely that not all the Member States have DPAs elected for at least five years. The five year long term of service will become even more problematic if the election process held by the European Data Protection Board does not coincide with the start of the term of a given DPA. Therefore, in our opinion, the term of service of the chair and two deputy chairpersons in the European Data Protection Board should be limited by their term of service as national DPAs.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Fragmentation of the data protection framework

The original aim of the Commission was to create “a comprehensive personal data protection scheme covering all areas of EU competence," which would "ensure that the fundamental right to data protection is consistently applied". Instead, however, the current proposals would perpetuate a seriously fragmented system of data protection rules (albeit with greater harmonisation in some areas):

- processing of personal data by private entities would be covered by the new Regulation, *except* that processing for “exclusively personal or household purposes” would remain fully exempt, and (more importantly) processing of important data such as traffic- and location data by e-communication service providers would continue to be covered by the (divergent) national laws implementing the e-Privacy Directive (Directive 2002/58/EC) (although the processing of other types of geolocation data by other controllers would be subject to the Regulation and not the e-Privacy Directive), and the rules on compulsory suspicionless retention of traffic- and location data would continue to be subject to the (equally divergent) laws implementing the Data Retention Directive (Directive 2006/24/EC;
- processing of personal data by public-law entities in the Member States in relation to matters covered by Union law would be covered by the new Regulation, ***except*** that processing by law enforcement agencies would be covered by the national laws implementing (undoubtedly in divergent ways) the proposed new Law Enforcement Data Protection Directive, and that processing by Member States in relation to the Common Foreign and Security Policy would be subject to whatever national laws would apply to that processing (if any);
- processing by EU institutions, bodies, offices and agencies would remain subject not to the new Regulation, but to Regulation (EC) No 45/2001 of 18 December 2000; and
- processing by Member States in relation to national security is and remains totally outside the scope of EU law, and thus also of the Regulation (and of the new Directive, or indeed any EU legal rules) (Art. 4(2) TEU).
- access to communications databases would be governed by national concepts of reasonableness and would result in entirely unpredictable access to databases covering data subjects in multiple jurisdictions.

The solution:

In our opinion, this continued fragmentation is neither necessary nor desirable. Intellectually and in terms of constitutional/fundamental rights law there is no reason why all processing of personal data subject to EU law should not be subject to one set of overarching basic rules. Moreover, the Regulation (including the restrictions and exemptions contained within it) is perfectly suitable to that end.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org

Relationship between the Draft Regulation and the e-Privacy- and Data Retention Directives

Summary of analysis

The issue:

Under the proposed Data Protection Regulation, the e-Privacy Directive and the Data Retention Directive (which is directly linked to the e-Privacy Directive) would remain in force, independent from the Regulation. Our analysis has shown that this would, if anything, amplify the existing problems with these two Directives:

- to the extent that one could derive at least some clarification and guidance on the interpretation of the e-Privacy Directive and the DRD from the provisions in the main Directive, this would be removed;
- the differences between the regimes for "ordinary" service providers and providers of e-communication service providers (in particular in respect of [geo]location data) would become even greater; and
- any flexibility in the Regulation to adapt to new technologies would be denied to processing under the e-Privacy Directive.
- Most crucially, the dis-application under the Data Retention Directive of the *caveat* in Article 13 of the main Directive relating to respect for fundamental rights, would become even more serious and sinister.

The solution:

We propose two simple steps:

1. That the e-Privacy Directive and the Data Retention Directive, to the extent that they will continue in force for the time being, be explicitly made subsidiary to the rules in the Regulation (including the exception and derogation clauses in the Regulation), and,
2. That within a very limited period, they be replaced by new rules that fit in with the new Regulation and that expressly and explicitly make the application of those new, subsidiary rules subject to the fundamental rights requirements of the Treaties.

This would mean first of all that ambiguous provisions in the two Directives can be simply applied in a manner consistent with the application of the main rules in the Regulation, and with the new guidance that will be provided under the Regulation by the Data Protection Board and the delegated acts of the Commission. Secondly, we believe that this would require the urgent replacement of the Data Retention Directive with a new legal instrument mandating only a Charter- and ECHR-compliant system of compulsory data preservation, of the kind we have long asked for. We believe the above would provide for major improvements in the overall EU data protection regime as currently applied to processing (and retention) of various types of communication and similar data.

European Digital Rights
Rue Belliard 20, B-1040 Brussels
Tel:+32 (0)2 274 2570
brussels@edri.org | http://www.edri.org