Data protection certificates and the competitive advantage of data protection law

Article · January 2021

CITATIONS
0

READS
45

1 author:

Max von Grafenstein
Einstein Center Digital Future
29 PUBLICATIONS **70** CITATIONS

SEE PROFILE

Contribution to the book:

"*Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*"
Hrsg.: Gloria González Fuster, Rosamunde van Brakel and Paul de Hert
Edward Elgar Publishing, as part of their series Research Handbooks in Information Law

Title:

Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design

Author:
Dr. Maximilian von Grafenstein LL.M.

1. Introduction

The European legislator has frequently stressed the competitive advantage that is provided in the upcoming General Data Protection Regulation (GDPR).[1] However, there is little scientific evidence as to whether this promise will come true or not. Focusing on data protection certification mechanisms, this paper illustrates why the regulatory approach inherent in the GDPR has indeed the potential to provide its regulation addressees, that are, data controllers and processors, competitive advantage and even enhance data-driven innovation. Therefore, this paper will first outline an approach that will help to conduct research on the effects of regulatory instruments on innovation. This perspective differentiates between two perspectives. In a first step, the approach assesses which regulatory instruments are best suited to protect the individuals against the risks caused by innovation. In a second step, the approach focuses on the question on how these risk protection instruments should be designed to not unnecessarily hamper innovation, or even enhance innovation. This two-levelled approach does not only help the legislator to draft laws that both effectively protect against risks *and* support innovators in their innovation processes, but the approach also helps interpret existing laws regarding both regulatory functions. In this regard, this paper will firstly demonstrate that a co-regulation strategy is particularly suitable for reaching this aim, and secondly that the GDPR can be interpreted in such a way that it does not only protect against data protection risks but, indeed, also provides for competitive advantages. This becomes clear, in general, when examining the effects of data protection certification mechanisms on a micro-, meso-, and macroeconomic level, if these mechanisms are used to specify and standardise, for example, the data protection- and security-by-design requirements (Art. 25 and 32 GDPR). Following the proposed levels at which the competitive advantage can be achieved, conclusions can be drawn, in particular, on the following aspects. Firstly, the different economic effects of data protection certification mechanisms compared to codes of conduct (and to a limited extent also to binding corporate rules — in the following also referred to as "BCR"). Secondly, the different incentives to specify and standardise the GDPR provisions that depend on the type of data controllers and processors. Third, the appropriate level of protection signaled by data protection certification mechanisms and its interplay with the "state of the art"-requirement. Fourthly, the suitable object of data protection certification mechanisms with respect to the ability of data subjects to assess the level of protection. Lastly, three selected key questions on how to cope with the complexity of such "data protection markets", taking into account the perspective of certification bodies, data controllers as well as processors, and data subjects. On this basis, the paper concludes by highlighting the need for empirical research to answer several remaining questions on the effectiveness of the discussed regulatory instruments from the point of view of regulating innovation.

[1] See, instead of many other statements, the "Statement by Vice President Neelie Kroes ,on the consequences of living in an age of total information'" from the 4th of July 2013, (Sep. 30, 2017), http://europa.eu/rapid/press-release_MEMO-13-654_en.htm; see also, the German discussion, for example, Roßnagel (1997) DuD 505 (514); Helmut Bäumler, Albert von Mutis `Datenschutz als Wettbewerbsvorteil` (1st edn, Vieweg+Teubner Verlag, 2002).

2. Regulating data-driven innovation: Stuck in a regulatory dilemma?

To answer the question under which conditions the GDPR can lead to a competitive advantage, this paper builds on the research approach of regulating innovation. From the regulator's point of view, this approach raises two fundamental questions: First, which regulatory instruments protect best against the risks caused by innovation; and second, among those instruments, which hinder the innovation processes of the regulation addressees the least, or can even enhance innovation.[2] From this perspective, the law as such is not an inherent barrier to innovation, but rather a leveller of innovation.[3] In fact, under which conditions a law protects, effectively, individuals against risks caused by innovation and under which conditions this does not unnecessarily hinder innovation processes, or even enhances such processes, cannot be answered by legal research alone. Instead, in order to do research on the effects of regulatory instruments, it is necessary to build upon other (in particular, economic) research disciplines by using their concepts, theories and (in particular, empirical) research methodologies.[4] With these considerations in mind, the next few sections show why the upcoming General Data Protection Regulation provides a set of instruments that are, in principle, well-suited for the regulation of data-driven innovation, and could indeed provide a competitive advantage.

2.1 Knowledge uncertainty as an inherent element of innovation

The approach of regulating innovation understands knowledge uncertainties as an inherent element of innovation processes. Schumpeter was one of the first economists to recognize innovation as a key driver of social change. In doing so, he contradicted the prevailing view on price competition as the primary economic force. Instead, Schumpeter identified "the new consumers' goods, the new methods of production or transportation, the new markets, the new forms of industrial organization that capitalist enterprise creates" as the essential impulse "that sets and keeps the capitalist engine in motion".[5] Focusing on the "entrepreneur" as the actor who brings such innovations to the market, Schumpeter stressed the "function of entrepreneurs (...) to reform or revolutionize the pattern by exploiting an invention or, more generally, an

[2] See Wolfgang Hoffmann-Riem, Innovationsoffenheit und Innovationsverantwortung durch Recht – Aufgaben rechtswissenschaftlicher Innovationsforschung (Openness toward Innovation and Responsibility for Innovation by means of Law), in: Archiv des öffentlichen Rechts 123 (4) 513–540 (1998).

[3] See Viktor Mayer-Schönberger, The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship, 6 (2) 159-169 (2010); Urs Gasser, Cloud Innovation and the Law: Issues, Approaches, and Interplay, No. 2014-7 19-20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410271>

[4] See Wolfgang Hoffmann-Riem, Saskia Fritzsche, Innovationsverantwortung - Zur Einleitung, 39, in: Martin Eifert, Wolfgng Hoffmann Riem (eds.), Innovations und Recht III - Innovationsverantwortung, 11-41, (Duncher & Humboldt, 1st ed., 2009)

[5] See Joseph Schumpeter, Capitalism, Socialism & Democracy, 82-83 (5th ed. 2003).

untried technological possibility for producing a new commodity or producing an old one in a new way (...) and so on."[6]

From such an understanding of *evolutionary* markets, the approach of regulating innovation takes it as a matter of fact that the regulator has limited knowledge about future events.[7] Focusing on risks, as one side of the "innovation coin", there has been an intensive – and still ongoing– debate on how to define risks. Especially in the German environmental protection law debate, the discussion has focused, mainly in the 80s, on clarifying the different terms of "risks" and "dangers" that were, more and more, parallel used in laws. Pursuant to sociological approaches, the term "risk" aims to make an incalculable danger calculable. Thus, the specific knowledge about the probability and severity of a "danger" makes this danger a "risk".[8] In the German legal discussion, however, both terms have been actually used for nearly a century in the opposite sense: a "danger" is referred to as the calculable threat, whereas "risk" is used to refer to a situation where there is not enough knowledge about whether a certain action leads to harm for a specific object of protection.[9] However, this short summary of the discussion does not aim to decide in favour of the one or the other definition. Rather, the aim is to demonstrate that the legal discussion has implicitly acknowledged that the regulator is confronted with different types of threats resulting from different types of knowledge uncertainties: on the one hand, there are situations where it is possible to say, with a certain degree of probability, that a certain action can lead to harm for a specific object of protection; on the other hand, there are situations in which there is not enough knowledge about such a

[6] See Schumpeter, ibid., p. 132.

[7] See Wolfgang Hoffmann-Riem, Saskia Fritzsche, ibid., pp. 259-262; Ivo Appelt, Aufgaben und Verfahren der Innovationsfolgenabschätzung (Tasks and Procedures of the Innovation Impact Assessment), in: Martin Eifert, Wolfgang Hoffmann-Riem, Innovation und Recht III – Innovationsverantwortung, 147–181 (149) (Mohr Siebeck, 1st ed., 2009); cf., regarding technology regulation, Charles D. Raab and Paul De Hert, Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood, in: Roger Brownsword, Karen Yeung (eds.), Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes, 263–285 (2008); concerning cyber regulation, Andrew Murray, Conceptualising the Post-Regulatory (Cyber)state, in: Roger Brownsword, Karen Yeung (eds.), ibid., 287–316 (2008); further developed: Andrew Murray, The Regulation of Cyberspace – Control in the Online Environment In: Modern Law Review 70, (5) 879–883 (2007); and with respect to regulation *per se*, Robert Baldwin, Martin Cave, Martin Lodge, Understanding Regulation – Theory, Strategy and Practice, (2nd ed.) (2013); Claudio Franzius, Modalitäten und Wirkungsfaktoren der Steuerung durch Recht (Modes and Impact Factors for the Control through Law), § 4, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012); see also Martin Eifert, Reguierungsstrategien (Regulation Strategies), in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012)

[8] See Liv Jaeckel, Gefahrenabwehrrecht und Risikodogmatik – Moderne Technologien im Spiegel des Verwaltungsrechts (Prevention of Danger through Law and Legal Conceptualization of Risk), 51- 52, (Mohr Siebeck, 1st ed., 2010), by referring to Adalbert Evers, Helga Novotny, Umgang mit Unsicherheit, (Suhrkamp, 1st ed., 1987); cf. also Raphael Gellert, Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative, 7-13, in: International Data Privacy Law, 5 (1), 3-19, (2015); referring to Patrick Peretti-Watel, La société du risque (Repères. La Découverte, 1st ed.2010); Olivier Borraz, Les politiques du risque (Presses de Sciences Po, 1st ed., 2008), Jenny Steele, Risks and Legal Theory, (Hart Publishing, 1st ed., 2004) 21, Jacqueline Peel, Science and Risk Regulation in International Law, 79-80 (Cambridge University Press, 2010).

[9] See Jaeckel, ibid., pp. 52 and 55-56.

linear causal-effect-relationship, but the mere possibility of harm is already sufficient to justify a (precautionary) protection.[10]

The same differentiation of knowledge uncertainties can be observed when the regulator's perspective is changed to the perspective of innovative entrepreneurs as the addressees of the regulation. Economists essentially conceptualise, an entrepreneurial process as a bundle of the following activities: locating business opportunities, accumulating resources, and building organizations in order to produce market products or services, while constantly interacting within the entrepreneurial environment.[11] What matters here is how economists look at the way entrepreneurs locate their business opportunities. In this regard, two main theories are relevant here: The Discovery Theory and the Creation Theory. The first theory says that an entrepreneur "discovers" an already existing business opportunity, building on the situation where an entrepreneur has sufficient knowledge about a specific outcome of his or her actions. Such an entrepreneur cannot be completely sure about the outcome but he or she can at least expect it with some probability.[12] In contrast, the Creation Theory refers to a situation where an entrepreneur does not have enough knowledge of the likelihood of a particular outcome. In this case, economists stress that "entrepreneurs maximize their probability of success by (1) engaging in iterative, incremental, and inductive decision making, (2) developing very flexible and constantly adjusting business plans"[13] and generating "resources that, from the point of view of potential competitors, are intractable (...) and causally ambiguous (...)."[14] This second theory is particularly relevant in innovative, highly dynamic, non-linear environments.[15]

So far, this section has shown that both the regulator and the regulation addressees face the same knowledge uncertainties in highly dynamic, innovative environments. Given the described knowledge uncertainties, the question arises as to which regulatory instruments are most suitable for an effective regulation.

2.2 Openness of regulatory instruments to innovation (e.g. legal principles and broad legal terms)

Legal scholars have long been debating the appropriate functions, modes, and strategies that could be considered for an effective regulation in complex, highly dynamic, innovative environments. Even if the debate does not always use the same terminology, the common

[10] See Jaeckel, ibid., 69-81; cf. Luiz Costa, Privacy and the precautionary principle, 14-19, in: Computer Law & Security Review,14-24 (2012).

[11] See, for instance, William B. Gartner, A Conceptual Framework for Describing the Phenomenon of New Venture Creation, p. 702, in: The Academy of Management Review 10 (4) 696-706 (1985)

[12] See Sharon Alvarez, Jay B. Barney, Discovery and Creation: Alternative Theories of Entrepreneurial Action, 13 in: Strategic Entrepreneurship Journal 1 (1) 11-26 (2007).

[13] See Alvarez and Barney, ibid., p. 32.

[14] See Alvarez and Barney, ibid., pp. 36-37.

[15] See Alvarez and Barney, ibid., pp. 33-34, regarding the knowledge uncertainties, and regarding the non-linearity of innovative environments, Jan Fagerberg, Innovation: A Guide to the Literature, Box 1.3 „What innovation is not: the linear model", 11, in: Jan Fagerberg, David C. Mowery (eds.), The Oxford Handbook of Innovation (Oxford University Press, 2004)

starting point, as previously described, are the knowledge uncertainties of the actors involved in these environments.[16] As one of them, Eifert determines the regulatory strategies for the role a State plays within a regulatory complex field, differentiating between imperative law ("command and control", often also referred to as "rules), state-regulated self-regulation ("co-regulation", also described as "principles" or "standards"), and social self-regulation. Focusing on imperative law (command-and-control) and instruments of regulated self-regulation (co-regulation),[17] Eifert provides a useful summary of the advantages and disadvantages of these two types of regulation:

A command-and-control regulation provides for a high degree of legal certainty given the clarity of the "if-then"-rules and a more direct form of execution. However, this type of regulation can be inefficient because it does not take the specific circumstances of the regulation addressees and the constraints of their economic behaviour into account. The inflexibility of this type of regulation can severely restrict their room of action because they cannot react to and adapt to the dynamic changes in the environment, when they want to meet the regulatory expectations. Therefore, the more knowledge the regulator has of the effectiveness and efficiency of its protection instruments, the more appropriate this type of regulation will be. On the other hand, if the regulator does not have sufficient knowledge, such as in complex, highly dynamic, innovative environments, this type of command and control regulation does not provide the most appropriate instruments.[18]

Regarding complex, dynamic and innovative environments, Eifert instead emphasises co-regulation as the more appropriate regulatory strategy. The main reason for this is that this strategy can can build much better on the decentralised knowledge of private entities in order to react more specifically to the particularities of certain environments.[19] As mentioned above, in innovative environments, legislators lack sufficient knowledge to pinpoint the circumstances of the entrepreneurial activities and the impact of these activities on individuals. Precise (if-then) rules therefore carry the risk of over-regulation and of ineffectively addressing the actual threat. Therefore, the regulator may decide to establish legal principles and/or broad legal terms so that the regulation addressees have more room to find the best solution by themselves to achieve the regulatory objective.[20] Since this strategy is based on the decentralised knowledge of all regulation addressees, it potentially increases the problem-

[16] Cf. Robert Baldwin, Martin Cave and Martin Lodge, ibid.; Charles D. Raab and Paul De Hert, ibid., ; Andrew Murray, ibid.; Claudio Franzius, ibid.

[17] See Martin Eifert, ibid., cip. 13 to 15; focusing on privacy-related principles; Winston J. Maxwell, Principles-based regulation of personal data: the case of ‚fair processing, in: International Data Privacy Law, 205–216, 5 (3) (2015), referring to Julia Black, Forms and Paradoxes of Principles Based Regulation', in: Capital Markets Law Journal, 3 (4), 425-457 (2008); , Louis Kaplow, Rules Versus Standards: An Economic Analysis, in: Duke L. J. 42 (3) (1992); Richard A. Posner, Economic Analysis of Law, 747. (Aspen/Wolters, 8th ed.).

[18] See Martin Eifert, ibid., cip. 25-26; cf, focusing on "privacy seals": Rowena Rodrigues, David Wright, Kush Wadhwa, Developing a privacy seal scheme (that works), 109-110, in: International Data Privacy Law, 3 (2), 100-116 (2013)

[19] See Martin Eifert, ibid., cip. 59; cf. Rowena Rodrigues, David Wright, Kush Wadhwa, ibid., 110-111

[20] Cf. Martin Eifert, ibid., cip. 25-26; Claudio Franzius, ibid., cip. 7, 17, 81-103; Charles D. Raab and Paul De Hert, ibid., p. 278; focusing on the technological neutrality of data protection law, Irene Kamara, Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate, in European Journal of Law and Technology, 8 (1), 8-11, (2017)

solving skills in society. Since this strategy is based on the logic of entrepreneurial behaviour, its regulatory instruments are — at least in principle — also more effective.[21]

Keeping these different regulation strategies in mind, a closer look at the General Data Protection Regulation shows that the legislator has obviously opted, at least to a substantial extent, for a principle-based approach. This applies at least to the processing principles under Art. 5 GDPR, as well as the data protection and security-by-design requirements under 25 and 32 GDPR. In doing so, the legislator has combined, with particular respect to Art. 5 and Art. 25 GDPR, two approaches with each other, the so-called rights-based approach (as enshrined in Art. 5 GDPR) and the so-called risk-based approach (as stated in Art. 25 GDPR). There are several commonalities and differences between the two approaches.[22] However, what is most relevant for this contribution, is how the legislator has combined the principles under Art. 5 GDPR, which are applicable to all kind of processing of personal data, with the risk-based approach under Art. 25 GDPR that enables the regulation addressee to take the contextual particularities into account. Pursuant to Art. 25 GDPR, the data controller has to implement the principles listed in Art. 5 GDPR by taking, among other aspects, the "risk", "purpose" and "context" of its processing into account. While all these legal principles and terms are rather broad and vague, the advantage of this combined approach is that the regulation addressees have both a normative direction and enough leeway to find solutions that best fit the regulatory goal, taking into account the specifics of their entrepreneurial processing context.[23]

2.3 Legal uncertainty as a hindering factor for innovation

One particular drawback of such broad and vague provisions is, in general, that the way a regulatory addressee applies the law may not be in line with the regulator's expectations.[24] There may be two different scenarios in this regard: In the first scenario, the regulation addressee really wants to meet the regulatory aim, but does not succeed because he or she does not know what the regulator is explicitly expecting from them. In the second scenario, the addressee actually does not want to meet the regulator's expectations and uses the broadness and vagueness of the legal provisions as a loophole, abusing its advanced knowledge about its specific entrepreneurial circumstances to the detriment of the individuals concerned. This might be the case, for instance, if the regulator grants these entrepreneurs privileges because it believes that their solutions serve the persons concerned, but in reality, only serve their

[21] See Martin Eifert, ibid., cip. 59.

[22] Comparing both approaches in detail see: Raphael Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection, in: European Data Protection Law Review (EDPL), 4 (2), 481-292, (2016).

[23] See, in more detail, Max v. Grafenstein, The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation, in particular, pp. 508-590, (Mohr Siebeck,1st ed., 2018, to be published)

[24] See Martin Eifert, ibid., cip. 60; cf. Rowena Rodrigues, David Wright, and Kush Wadhwa, ibid., pp. 110-111, focusing on self-regulation of "privacy seals".

business interests.[25] In the first scenario, legal uncertainty negatively affects the innovative entrepreneurs, and in the second scenario, the individuals concerned.

This fact leads to a regulatory dilemma in innovative environments. On the one hand, if the regulator provides for specific rules, these rules run the risk of over-regulation and of not meeting the actual threat that is caused by innovation. On the other hand, if the regulator provides for broad legal terms and/or principles that are basically open toward innovation (because innovative entrepreneurs are able to adapt these legal requirements to the particularities of a specific case), this reduces legal certainty.

3. Escaping the dilemma: Co-regulation and specifying standards

In order to solve this conflict between legal principles and/or broad legal terms, which are open to innovation, and legal uncertainty, the regulator can add procedural instruments enabling the regulation addressees to increase legal certainty on their own. A prominent example are standards that are set up by private entities, by involving to some extent the regulator, that specify the law in regards to technical and organisational requirements.[26] Such a combination of legal principles or broad legal terms with procedural instruments is typical for a co-regulation strategy. With respect to the described knowledge uncertainties, such a strategy is particularly useful for assessing the risks caused by innovation because it enables the regulation addressees to take the particularities of their specific context into account, whether in relation to a particular product or service category, or a certain type of processing activity.[27] However, the next sections will focus on the other side of the "innovation coin". Thus, the question concerns the conditions under which these risk-protection instruments can not only

[25] See Martin Eifert, ibid., cip. 60; see also Irene Kamara, ibid., p. 4, referring, on the one hand, to Colin J. Bennett, Charles D. Raab 'The Governance of Privacy: Policy Instruments in Global Perspective' 155, (MIT Press, updated paperback ed., 2006) and on the other hand, to Dennis D. Hirsch, 'In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct' in: Ohio St. LJ, 74 (6), 1029 (1043), (2013)

[26] See, for example, the International Organization for Standardization (ISO) and the International Electrotechnical Commission of Standardization (IEC) defining a "standard" as a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context", under http://www.iso.org/sites/ConsumersStandards/1_standards.html, (re-called 20 January 2017); see for further definitions, Paul de Hert, Vagelis Papakonstantinou, Irene Kamara, The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection, 18, in: Computer Law & Security Review 32 (1), 16-30,

[27] See Martin Eifert, ibid., cip. 59; cf. also Irene Kamara, I., ibid., pp. 13-14, who discusses the issue taking the example of the European Commission's privacy by design standardisation request with regard to European data protection law. However, this perspective is, in the view of the author of this contribution, not sufficiently context-specific to properly address the context-dependency of data protection risks; in contrast, see the considerations regarding the ISO Cloud Standard at Paul de Hert, Vagelis Papakonstantinou, Irene Kamara, ibid., p. 27, which seems therefore to be a better example in this context.

be opened up for innovation, but even enhance innovation and market competition.[28] In this regard, the first part focuses on the microeconomic level on how increasing legal certainty can have a positive effect on entrepreneurial activity. At the mesoeconomic level, the second section concentrates on the positive impacts of standards on the decisions of consumers or business customers purchasing innovative products or services. Finally, the third section gives an outlook on how this kind of regulation can have positive effects on the innovation capacity of a market as a whole.

3.1 Reducing the complexity of an entrepreneurial process (microeconomic level)

To understand the effects of standards on the microeconomic level, one must first look more closely at the effects of legal certainty and uncertainty on entrepreneurial activity. Authors in the economic discipline see high legal certainty as an enhancing factor rather than a hindrance to doing business. The reason for this is that the law does not only limit the room for maneuver of an entrepreneur but also helps him or her to defend and enforce legal claims.[29] However, some studies show that legal certainty tends to help large enterprises rather than small and medium-sized companies.[30] Levie and Autio explain this observation, bearing in mind that smaller companies usually have "disproportionately high compliance costs, because their small initial size makes it costly for them to maintain compliance functions internally. For industry incumbents, whose large size permits a greater degree of internal specialisation and the maintenance of a larger administrative function in absolute terms, compliance costs are less significant."[31] However, the study by Levie and Autio demonstrate that if the regulatory burden is low, companies (not just large but also small and medium-sized companies) can benefit from a high level of legal certainty.[32] In this case, "([B]ureaucracy and red tape [do not] hamper entrepreneurial growth and divert scarce resources of potentially high-growth entrepreneurial firms away from their core business".[33]

This last consideration leads to the reason why an increase of legal certainty can be a factor in enhancing innovation (given a low regulatory burden): Legal certainty can be an enhancing factor for entrepreneurial activity, because entrepreneurs generally prefer, given the high level of uncertainty they face during their innovation processes, to know exactly what the

[28] Cf. with respect to the effects of technical standards on innovation, Knut Blind, The Impact of Standardization and Standards on Innovation., in: Manchester Institute of Innovation Research (ed.), Compendium of Evidence on the Effectiveness of Innovation Policy Intervention, (2013), availabe under <http://www.innovation-policy.org.uk/compendium/section/Default.aspx?topicid=30.>

[29] See, for example, Chantal Hartog et al., Institutions and Entrepreneurship: The Role of the Rule of Law, 8. (7 January 2018), http://ondernemerschap.panteia.nl/main/publication/bestelnummer/h201003

[30] See Hartog et al., ibid., p. 3.

[31] See Jonathan Levie, Erkko Autio, Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, 1411. in: Journal of Management Studies 48 (6) 1392–1419 (2011)

[32] See Levie and Autio, ibid., pp. 1400-1401.

[33] See Levie and Autio, ibid., p. 1411.

regulator expects from them.[34] Mayer-Schönberger sums up this point of view by arguing that "the role of the legal system in facilitating entrepreneurial activity is to reduce the uncertainties that entrepreneurs perceive."[35] Mayer-Schönberger also draws several conclusions from this function of the law: Empirical studies show that individuals are more risk-averse, the higher the final payoff. Thus, he proposes, for example, to increase legal certainty when entrepreneurs face high profits or costs. Second, as individuals are more risk-averse when they evaluate profits and more risk-taking regarding eventual losses, Mayer-Schönberger suggests "that lawmakers should focus on making legal rules more certain for financial benefits offered to entrepreneurs, like subsidies, rather than costs, like taxes".[36]

From this perspective, the law does indeed not hinder innovation, but can rather serve as a business opportunity: Tied to the entrepreneurial Discovery Theory, the regulation strategy of "command-and-control" provides entrepreneurs with precise criteria for applying the law. Entrepreneurs must "discover" these criteria and organise their processes according to these criteria in a "causal-linear" way. In highly dynamic, innovative environments, however, this regulatory strategy runs the risk of unnecessarily increasing bureaucracy and hindering entrepreneurial activity. Therefore, the regulator can also build on the logic of the Creation Theory by establishing legal principles and/or broad legal terms and, in addition, procedural mechanisms that allow entrepreneurs to specify these norms for themselves. As such procedural instruments, data protection certification mechanisms established under Art. 42 and 43 GDPR, as well as codes of conduct pursuant to Art. 40 and 41 GDPR, can be introduced because they enable data controllers and processors to specify and standardise the legal principles and broad legal terms, thus increasing legal certainty.[37] Entrepreneurs can use these mechanisms to ensure that the way they specify the legal principles and broad legal terms really meets the regulators' expectations. To summarise, this regulatory strategy is not only open to innovation but has also the potential to enhance entrepreneurial innovative capacities.

3.2 Signalling a certain level of protection to market participants (mesoeconomic level)

Moreover, such a co-regulation strategy can also have positive effects on a mesoeconomic dimension. By laying down legal principles and broad legal terms, the regulator leaves data controllers and processors sufficient room for their specific application. This, in turn, leads to a variety of possible solutions.[38] From the point of view of New Institutional Economics, Wegner

[34] Cf. also Kloepfer, Law enables Technology – About an underestimated function of environmental and technology law, 417-418, in: Natur und Recht 417–418 (1997).
[35] See Mayer-Schönberger, ibid., pp. 177-178.
[36] See Mayer-Schönberger, ibid., pp. 179-180.
[37] See, for example, Stefan Heilmann, Wolfgang Schulz, ibid., Art. 40, cip. 1, and Art. 42, cip. 2; however, see Eric Lachaud, The General Data Protection Regulation and the rise of certification as a regulatory instrument, in: Computer Law and Security Review (March 2017), who argues that the data protection certification mechanisms have to be categorised under a new category called "monitored self-regulation".
[38] See Gerhard Wegner, Nachhaltige Innovationsoffenheit dynamischer Märkte (Dynamic Markets and their Persistent Openness to Innovation), 74-75, in: Martin Eifert, Wolfgang Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 71-91, (Duncker & Humblot, 1st ed. 2009).

demonstrates under which circumstances the regulator can enable such market creativity.[39] He explains that given the evolutionary nature of innovations, such market creativity depends on how quick the entrepreneurs react to constant changes in their respective environments. From this economic point of view, the best that a regulator can actually do is to guarantee the existence of fair competition in the markets, as well as guaranteeing that the entrepreneurs participating in a market can make autonomous decisions. If, on the other hand, the legislator requires entrepreneurs to apply a regulatory objective in a specific way it minimises their entrepreneurial capacity to innovate and, thus, the variety of possible solutions overall.[40] From this (economic) perspective, the regulation "command-and- control" strategy (also) is, therefore, less able to uphold market creativity than a co-regulation strategy containing the provision of legal principles and broad legal terms.[41]

On this basis, consumers decide for or against certain products or services of specific qualities that determine the success of entrepreneurial, innovative activities. In terms of data protection law, this means that data subjects must be able to choose which product or service of certain "data protection qualities" they prefer: Data subjects who prefer a lower data protection level (for instance, for a cheaper price) do not have to buy products or services with a higher protection level (hence, for a probably higher price).[42] A data controller can thus determine the quality of (data) protection of a specific product or service, whether with the involvement of the regulator (co-regulation) or without it (self-regulation). The standardisation of such a product or service quality, for example, in the form of a certificate, then signals this level of protection to the data subject.[43]

There are also some pitfalls in this concept, for example when the transaction costs of the consumers are too high to verify the "data protection quality" of a certain product or service in question. This may be the case if there is no common scale that is actually necessary in order to compare the differences in quality. This can be particularly relevant with respect to the so-called risk-based approach.[44] The risk-based approach is an essential element, for example, of

---

[39] See Wegner, ibid., p. 73.

[40] See Wegner, ibid., pp. 74-80.

[41] Cf. already the regulatory perspective focusing on the regulator's knowledge deficiencies, above under point "Knowledge uncertainty as an inherent element of innovation".

[42] Cf. Wegner, ibid., pp. 84-85; in contrast, many authors mainly consider the compliance function of Art. 42 and 43 GDPR (which was discussed in the previous section), for example, ENISA, Recommendations on European Data Protection Certification, Version 1.0, 13, (November 2017); Rowena Rodrigues, David Barnard-Willsa, Paul De Hert, Vagelis Papakonstantinou, The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, 249, in: International Review of Law, Computers & Technology, 30 (3), 248–270, (2016), available under: < http://dx.doi.org/10.1080/13600869.2016.1189737>; however, see Rowena Rodrigues, David Wright, and Kush Wadhwa, ibid., p. 105, who also considers, beside the compliance function, the additional goal "to ensure a higher level of protection for individuals".

[43] Cf. Wegner, ibid., pp. 85-86; Roßnagel, Data protection in computerized everyday life, 195, (2007), http://library.fes.de/pdf-files/stabsabteilung/04548.pdf; critical regarding such a competition amongst certification bodies, Rowena Rodrigues, David Barnard-Wills, Paul De Hert & Vagelis Papakonstantinou, ibid., p. 263.

[44] Cf. the risk-based approach regarding Directive 95/46/EC, Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks,, 14/EN, WP 218, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, 30 May 2014; regarding the DPIA under Art. 35 GDPR, ibid.,

the data protection and security-by-design requirements under Art. 25 and 32 GDPR. The risk-based approach requires data controllers and partly processors to implement data protection measures according to the specific risks.[45] Consequently, the "data protection quality" also depends on the risk measurement. So, if there is no common scale to measure data protection risks, it will not be possible for data subjects to compare products or services of different "data protection quality".[46] Another pitfall refers to the situation where the market for a certain product or service is so fragmented that the data subject loses the overview even if there was a common scale that makes a comparison of products possible.[47] This may be the case, for example, if there are too many data protection certificates on the market and the data subjects are overwhelmed by the variety. However, the guiding principle should be clear that a co-regulation strategy that provides controllers and processors with the ability to specify and standardize legal requirements can, at least in principle, strengthen the competition in a market and, consequently, market creativity because they can signal the data protection quality (of their specific product or service) to the data subject (i.e. consumer). Users of such a standard which signal a certain (data protection) quality of a specific product and/or service (for example, by using a data protection certification mechanism, pursuant to Art. 42 GDPR) can thus turn the room for maneuver that is laid out by law into a competitive advantage.

3.3 The "state of the art" as a driver of market innovation (macroeconomic level)

Last but not least, there is another related factor that can enhance the innovative capacity of a market on the macroeconomic level. This factor does not result from the standardisation *per se* of legal requirements, but rather from a particular element of the data protection and security-by-design requirements under Art. 25 and 32 GDPR. Both provisions require data controllers, and partly processors, to take the "state of the art" into account when implementing appropriate technical and organisational measures to mitigate the risks caused by their data

17/EN WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, ec.europa.eu/newsroom/document.cfm?doc_id=47711, (4 April 2017); Friedewald et al., Forum Privatheit, White Paper Datenschutz-Folgenabschätzung.,: http://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf, (2017); see also the internet knowledge base of the CNIL https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

[45] See Jana Moser, Art. 25, cip. 59 ff.; Johann Jergl, Art. 32, cip. 21 ff., in: Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel, Winfried Veil, Kommentar Datenschutz-Grundverordnung,, (Bundesanzeiger Verlag, 1st ed, 2017); comprehensively, regarding the risk-based approach of the GDPR, Winfried Veil, ibid, Art. 24, cip. 78-190

[46] In the opinion of the author of this contribution, the discussion on the data protection risk assessment methodology has not yet reached a level at which data subjects can reliably assess data protection risks and are able to compare, on that basis, different levels of data protection provided for by a certain processing operation. Given that data-driven products build on a whole bundle of processing operations, the data subjects are even less able to assess the level of protection of these products.

[47] See Wegner, ibid., pp. 80-82; cf., Rowena Rodrigues, David Barnard-Wills, Paul De Hert, Vagelis Papakonstantinou, ibid., p. 263.

processing activities. Legal scholars determine the nature of this term (i.e. the "state of the art") as an "undetermined legal concept".[48] To specify this legal concept, legal scholars in Germany refer to the same terms and related terms that are already used in other regimes, such as environmental and technology laws. In doing so, they define the term "state of the art" as the "best available technology".[49] The legal meaning of this term can be located between the following two related notions on a normative level: the "generally accepted rules of technology" (in German: "allgemein anerkannte Regeln der Technik") and the "state of science and technology" (in German: "Stand der Wissenschaft und Technik"). While the first notion provides for a lower level of protection, the second notion leads to a higher protection level than indicated by the term "best available technology". The reason for this is that the notion "generally accepted rules of technology" only requires that a certain technology must be approved in practice and accepted amongst the majority of experts. The technology does, therefore, not have to be the "best" technology available. In contrast, the notion "state of science and technology" requires, at least in principle, a higher level of protection since the obligation to use such a technology does not depend on its market availability.[50] This comparison may convey to the reader what it means when the term "state of the art" is interpreted as "best available technology".

Regardless of the precise meaning, legal scholars agree on the dynamic function of this reference.[51] At a first view, such a dynamic reference can serve as an innovation-enhancing factor on the market because it requires data controllers (and partly processors) to *constantly* adapt their protection measures to the "state of the art", which can *constantly* evolve.[52] The second view on behavioural dynamics, however, shows significant pitfalls of the regulatory concept behind such a dynamic reference.[53] In particular, the economist Gawel notes that this requirement actually deprives many regulation addressees of the incentive to innovate (i.e. to further develop the "state of the art"). Following the logic of the market economy, the main reason for this is that entrepreneurs will only advance a certain state of the art if it helps them to position themselves on the market with a higher "data protection quality" than their competitors do. However, as soon as all competitors are required to equally provide for this higher product or service quality, the innovator loses its competitive advantage and thus its business opportunity. The dynamic function of this reference thus leads to the situation where the innovator can no longer refinance development costs for its higher "protection quality". The result of this dynamic is that the "state of the art" requirement provides an incentive for the

[48] See Art. 25 cip. 38-42.

[49] Cf. Art. 3 Nr. 10 RL 2010/75/EU; see at Mario Martini, Integrierte Regelungsansätze im Immissionsschutzrecht, 210 and subs., (C.H. Beck, 1st ed., 2000); Ulrich Baumgartner, Tina Gausling, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, in: ZD 2017, 308.

[50] Cf. Jarass, BImSchG, § 3, cip. 92-96.

[51] See, instead of many other authors, Paal/Pauly, Datenschutz-Grundverordnung, DS-GVO Art. 32, cip. 56-59; in contrast, much less optimistic, see Lee A. Bygrave, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, 117 et seq., in: Oslo Law Review, 4 (2), 105-120, (2017)

[52] Cf. Paal/Pauly, Datenschutz-Grundverordnung, DS-GVO Art. 32, cip. 56-59.

[53] See the summary at Eric Gawel, Technologieförderung durch „Stand der Technik": Bilanz und Perspektiven, 216, in: Martin Eifert, Wolfgang Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 197-220, (Duncker & Humblot, 1st ed. 2009) 216; see, regarding further economic resistances, Lee A. Bygrave, ibid. p. 119.

addressees to hide. This is in particular the case with respect to the two following aspects: what the *actual* risk is that they may discover according to the particularities of their specific context; and what the appropriate measures of protection are that could *actually* be available in order to mitigate these risks. This regulatory approach, therefore, often leads to the opposite of what the regulator wants to achieve. Instead of the fact that the regulation addressees innovate and, what is equally important, reveal the information about such an innovation to others, it leads to a so-called "cartel of silence" because pushing a "state of the art" means investing without return opportunities.[54]

Garwel stresses that there are only a view factors that can break such a "cartel of silence" among the regulation addressees. The most important factor is a market participant that considers the further development of the "state of the art" as its core business "value proposition". Unlike the other regulation addressees, these market participants do not directly target the data subjects, whether they are consumers or business customers of data-driven products or services, but to other regulation addressees who in turn target the data subjects.[55] In this case, these market participants can use the legal requirement referring to the "state of the art" as a constantly renewed business opportunity because their business model relies on the legal obligation of the other regulation addressees: Each time these market participants push the "state of the art", they put the other addressees under pressure to implement the newly developed and now appropriate protection instruments. Coming back to Art. 25 and 32 GDPR, if the "state of the art"-requirement gets properly enforced,[56] this mechanism could well break the resistances of the "normal" regulation addressees.

4. Implications for the interpretation of the GDPR

In legal literature, there is a lively discussion on the pros and cons of different options of how to implement the co-regulatory instruments established under the GDPR, in particular, the data protection certification mechanisms of Art. 42 and 43.[57] This contribution does not aim to comment on all the questions that arose through the debate. a Instead, the purpose of this analysis is to determine how these provisions can be interpreted for the political promise to be fulfilled that the GDPR provides a competitive advantage. Based on the previous structure, the next sections will first address certain aspects regarding the function of increasing legal certainty with respect to codes of conduct and data protection certification mechanisms (and, to

[54] See Gawel, ibid., pp. 200-204.
[55] Cf. Gawel, ibid., p. 204.
[56] For example by data protection authorities on the basis of Art. 83 sect. 4 lit. a GDPR, or even by a data controller (or processor) as the "competitor" of the violating data controller (or processor) on the basis of §3a German Unfair Competition Act - see regarding the latter aspect, Gerald Spindler, Nationale Umsetzung der Datenschutzgrundverordnung im Bereich der Ko-Regulierung - Politikempfehlungen zur Schaffung rechtlicher Anreize für die Wirtschaft zur Entwicklung und Implementierung von Verhaltensregeln und Zertifizierungen, availabel under: https://sriw.de/images/pdf/2016-Gutachen-EU-DSGVO-SRIW---final_druc
k.pdf, (2016), who considers that the German Unfair Competition Act can be at least applicable if a competitor infringes the GDPR.
[57] See, for example, Rowena Rodrigues, David Barnard-Wills, Paul De Hert, Vagelis Papakonstantinou, ibid.; ENISA, Recommendations on European Data Protection Certification, Version 1.0, (November 2017).

a very limited extent, BCR). While data protection certification mechanisms refer to specific "processing operations by controllers and processors" (Art. 42 sect. 1 sent. 1 GDPR), codes of conduct are more generally related to "the specific features of the various processing sectors" (Art. 40 sect. 1 GDPR). Therefore, both mechanisms have different goals and can be used complementary to each other.[58] However, the following sections focus on specific questions with respect to data protection certification mechanisms. The last section will address issues of how to handle the complexity of this co-regulatory instrument.

4.1 Legal certainty function

This section compares codes of conduct and data protection certification mechanisms (and, to a very limited extent, BCR) with respect to its effects on increasing legal certainty. In this regard, the section also discusses how exactly these instruments should specify the law, and finally, various incentives for data controllers and processors to use these mechanisms.

4.1.1 Certification mechanisms and codes of conduct (as well as BCR)

Both codes of conduct and data protection certification mechanisms can reduce the complexity of entrepreneurial processes of the data controllers and processors by increasing legal certainty. In contrast, this function is limited with respect to BCR. In regards of codes of conduct and data protection certification mechanisms, this function is evident in several recitals. Recital 77 sent. 1 GDPR for example states:

> "*Guidance* on the implementation of appropriate measures and *on the demonstration of compliance by the controller or the processor*, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, *could be provided in particular by means of approved codes of conduct, approved certifications,* guidelines provided by the Board or indications provided by a data protection officer [emphasis added]."

With respect to the legal effects of complying with a data protection certification mechanism or code of conduct, recital 81 sent. 2 GDPR also stresses that:

> "The *adherence* of the processor *to an approved code of conduct or an approved certification* mechanism *may be used as an element to demonstrate compliance* with the obligations of the controller [emphasis added]."

Both mechanisms, therefore, intend to increase legal certainty with respect to either specific processing operations or, more generally, processing sectors. This legal-certainty-increasing

[58] See Stefan Heilmann, Wolfgang Schulz, Art. 42 GDPR, cip. 10, in: Sybille Gierschmann, Katharina Schlender, Rainer Stentzel Winfried Veil, Kommentar Datenschutz-Grundverordnung, (Bundesanzeiger-Verlag, 1st ed., 2017).

function becomes apparent in several provisions: Pursuant to Art. 24 sect. 3 GDPR, the application of codes of conduct or certificates "may be used as an element by which to demonstrate compliance with the obligations of the controller"; while only certificates can be used as an element to demonstrate compliance with the data protection-by-design requirement (Art. 25 sect. 3 GDPR), both certificates and codes of conduct can be used for demonstration purposes with respect to the security-by-design requirement (Art. 32 sect. 3 GDPR); both mechanisms can also help to demonstrate compliance with the necessary guarantees if personal data are processed on behalf of a controller or indirectly for another processor (Art. 28 sect. 5 GDPR); finally, certificates and codes of conduct can even help legitimise the transfer of personal data to a third country outside the EU (pursuant to Art. 46 sect. 2 lit. e and f GDPR). In all these cases, both mechanisms help to reduce the complexity of entrepreneurial data-driven processes. In contrast, the function of BCR are limited, in this regard, to only one of these aspects, that is, legitimising the transfer of personal data to a third country outside the EU (Art. 46 sect. 2 lit. b). In this contribution, however, BCR do not play a further role because of this limited functionality.

4.1.2 Degree of granularity of codes of conduct and certificates

So far, one conclusion can be drawn from the common function of increasing legal certainty on the level of granularity that is required for the specification of a code of conduct or certification mechanism. Both mechanisms can serve as an incentive for data controllers and processors to comply with the law by allowing them to specify broad legal terms and legal principles, thereby increasing legal certainty. At the microeconomic level, increasing legal certainty can, therefore, enhance the entrepreneurial innovation processes, as data controllers (and in some cases processors) can use the adherence to data protection certification mechanisms or codes of conduct as a means of demonstrating compliance with multiple requirements (pertaining to the legal principles or broad legal terms).[59] It must be stressed, however, that such a compliance function only works if the data protection certification mechanism or code of conduct indeed specifies the law, thus making it more specific.[60] For example, a data protection certification mechanism that specifies the data protection-by-design requirement for certain processing operations, must not simply repeat the legal text, in all its vagueness. Instead, such a data protection certification mechanism or a code of conduct may be more effective in exploiting the legal certainty increasing feature the more precisely it determines how this requirement is met with respect to specific processing activity. It is important to stress this aspect because previous examples have already shown that stakeholders who are involved in such a standardization process do not always make the law more specific.[61]

[59] Cf. above point "Reducing the complexity of an entrepreneurial process (microeconomic level)".

[60] Cf. Stefan Heilmann, Wolfgang Schulz, ibid., Art. 42, cip. 33, focusing on the control function; Matthias Bergt Art. 42 cip. 15, in: Jürgen Kühling, Benedikt Buchner, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz (CH. Beck, 2nd ed., 2018)

[61] See, for example, the code of conduct that was established in Germany by the Federal Insurance Industry Association (Gesamtverband der deutschen Versicherungswirtschaft e.V.), available under https://www.gdv.de/resource/blob/23938/8db1616525e9a97326e2f2303cf42bd5/download-code-of-conduct-data.pdf, which was set up under the application of § 38a of the German Federal Data Protection

In summary, the adherence to a data protection certification mechanism or code of conduct can demonstrate compliance with legal requirements more effectively, the more precisely the certification mechanism or code of conduct determines such a requirement. Conversely, if a data protection certification mechanism or code of conduct (or parts of it) simply repeat the legal text, its compliance function is zero.

4.1.3 Different incentives for different types of data controllers and processors

Another conclusion can be drawn regarding the incentives of data controllers and processors to reduce the complexity of their entrepreneurial processes.[62] If Mayer-Schönberger's conclusions are correct, the incentive to apply the law, given the opportunity to increase legal certainty, works best if data controllers (and partly, processors) face high benefits or costs. However, if they do not have much to lose or gain, the incentive will have less impact on an entrepreneur's decision to comply with data protection requirements. This means, for example, that a startup at an early stage of its development, which still operates on the basis of a low investment, will pay less attention to the possibility of increasing legal certainty. By contrast, the higher the investment or the chance of an economic breakthrough on the market, the more important the entrepreneurial opportunity to increase legal certainty becomes.[63] To make sure that an enterprise that still makes little investment, has an incentive to increase legal certainty (i.e. complying with the law), the regulator, such as a data protection authority, can still focus on fines. Although a potential loss through fines may be less effective than a potential gain as an entrepreneurial incentive to comply with the law, it is not ineffective.[64] In this respect, data controllers who follow an entrepreneurial approach can also use, their compliance to a data protection certification mechanism and/or code of conduct as an element in order to decrease the potential loss, i.e. a fine pursuant to Art. 83 sect. 2 lit. j GDPR.

4.2 Signalling function

This section discusses the effects of data protection certification mechanisms and codes of conduct on market competition with respect to their signalling function. Having first identified, in this regard, the main differences between certification mechanisms and codes of conduct, the following sections focus on certification mechanisms and discuss the level of protection that these mechanisms can signal on the market and the appropriate certification object.

Act (BDSG); in contrast, see the considerations regarding the ISO Cloud Standard at Paul de Hert, Vagelis Papakonstantinou, Irene Kamara, ibid., p. 27, which seems therefore to be a better example.

[62] See, in general, ENISA, ibid., p. 24, referring to Andrej Tomšič, Jelena Burnik, et al., 19, Consolidated report on enhancing confidence and acceptability of new certification measures., CRISP project, (2017)

[63] See above under point "Reducing the complexity of an entrepreneurial process (microeconomic level)", referring to Mayer-Schönberger, ibid., pp. 179-180.

[64] Cf. above under point "Reducing the complexity of an entrepreneurial process (microeconomic level)", referring to Mayer-Schönberger, ibid., pp. 179-180.

4.2.1 Differences between certification mechanisms and codes of conduct

In addition to the common function of increasing legal certainty, both mechanisms also show significant differences with respect to their effects on the mesoeconomic level. As explained earlier, standards can be used to signal to business customers and consumers the quality of certain data-driven products and services in terms of the level of data protection envisaged. Consumers and business customers can choose from a variety of products and/or services of different "data protection qualities" belonging to the same category; this, in turn, offers data controllers (and in part processors) the business opportunity to provide consumers or business customers with higher quality products or services who prefer such products or services to offers that belong to the same category but are of lower quality. In this regard, legal principles and broad legal terms, as discussed previously, combined with standardisation procedures that enable data controllers to specify the regulatory expectations, have the effect that data protection law can create a competitive advantage.[65]

However, as also shown above, this feature works only if different products or services belong to the same category but *can* have different data protection qualities. Only certificates can thus lead to such a competitive advantage at a mesoeconomic level, but not codes of conduct. The reason for this is that a code of conduct relates to a specific processing sector as a whole and, in principle, defines a common level of protection for all processing activities. As a result, all products and services in this sector provide the same level of protection. In contrast, certification mechanisms only apply to specific processing operations, not to one sector as a whole. As a result, products or services may belong to the same category but have different "data protection qualities". Unlike data protection certification mechanisms, codes of conduct do thus not give entrepreneurs the opportunity to offer higher quality products and/or services at a higher price, or of a lower quality and for a lower price.[66]

4.2.2 Level of protection signaled by data protection certification mechanisms

This difference between codes of conduct and data protection certification mechanisms leads us to the question whether it is, in fact, legally allowed that these certification mechanisms signal such a higher level of protection and, as a consequence, rely on criteria that are stricter than the level of protection provided for by law.

On the one hand, the wording of Art. 42 sect. 1 GDPR "(...) demonstrating compliance with this Regulation" seems to imply that data protection certification mechanisms should only demonstrate legal compliance but should not go beyond it by requiring from data controllers or processors a higher level of protection and signalling this to data subjects.[67] On the other hand,

[65] See above point "Signalling a certain level of protection to market participants (mesoeconomic level)".
[66] Cf. above under point "Signaling a certain level of protection to market participants (mesoeconomic level)", referring to Wegner, ibid., pp. 84-86; and Roßnagel, ibid., p. 195.
[67] See Patrick von Braunmühl, Art. 42, cip. 15 in Plath BDSG/DSGVO; Paal/Pauly, Paal, Art. 42, cip. 7; Gerrit Hornung, Korbinian Hartl, Datenschutz durch Marktanreize - auch in Europa? (Data Protection through Market Incentives – in Europe, too?), 224-225, In: ZD 4 (5) 219-225 (2014) .

some legal scholars argue that the law should not be interpreted too narrowly as the possibility of offering data protection certification mechanisms in the market with an even higher level of protection than provided for by law could increase competition in the market.[68] As described above, offering various data-driven products or services of different "data protection qualities" has indeed the potential to enhance competition on the market.[69] In fact, the wording of the law does not even prohibit different levels of protection as long as each level offered is within the scope of the law and, thus complies with it. Recital 100 GDPR also tends in this direction. This recital states that data protection certification mechanisms allow "data subjects to *quickly assess the level of data protection* of relevant products and services [emphasis added]." Of course, this wording, on the one hand, could simply lead to a certification mechanism helping, in any case, to assess the level of protection *quickly*, if ultimately only the same level of protection exists. As mentioned earlier, the assessment made by data subjects is likely to be faster if they can refer to a certification mechanism than without having such a signal as a basis for their purchasing decision.[70] On the other hand, the wording makes more sense if several products of the same category offer different levels of protection. The reason for this is that the assessment of the actual level of protection by data subjects is, in fact, superfluous if there is only one level of protection, that is, the level of protection provided for by law. Therefore, it is more plausible to interpret the law in such a way that it allows for different levels of protection.

However, it should be emphasised that there are, in fact, not many cases where it makes sense to discuss this question of different levels of protection. The reason for this is that the category of an equal level of protection does not match with the characteristics of a legal principle or broad legal term. As explained above, both legal instruments provide for regulatory objectives and leave, as its main characteristic, data controllers and processors enough room to find different ways of achieving these aims.[71] This essentially allows three different kinds of varieties: Firstly, different types of protection measures that are applied with regard to different risks (for example, on the one hand, special information against the risk of being manipulated by personalised marketing, and on the other hand, encryption measures against the different risk that communication will not remain confidential). Secondly, given one specific risk, there are several measures that ensure the same level of protection (such as a data protection authority or specialised private data broker, both acting on behalf of data subjects). Thirdly, a specific risk in which different types of measures result in different levels of protection (for example, opt-in instead of opt-out mechanisms). It only actually makes sense to talk about different levels of protection in this last case.

---

[68] See Stefan Heilmann, Wolfgang Schulz, ibid., Art. 42, cip. 34; Gerrit Hornung, Korbinian Hartl, ibid. p. 221; see also the argument at Eric Lachaud, Why the certification process defined in the General Data Protection Regulation cannot be successful, 820, in: Computer Law and Security Review, 32 (6), 814–826 (2016), that if there was only one level of protection, the use of data protection certification mechanisms would conflict with Provision 10 in Table 1 of the Directive 2005/29/EC ("Unfair Commercial Practices Directive"), which considers as unfair "Presenting rights given to consumers in law as a distinctive feature of the trader's offer."

[69] See above point "Signaling a certain level of protection to market participants (macroeconomic level)".

[70] See above point "Signaling a certain level of protection to market participants (macroeconomic level)".

[71] See above point "Openness of regulatory instruments to innovation".

Even if the same risk were present and data protection certification mechanisms could require a higher level of protection from the data controllers and/or processors and would be allowed to signal this to data subjects, the "state of the art"-requirement further restricts these (potentially) competition-enhancing effects. The reason for this is that the data protection and security-by-design requirements oblige the regulation addressees to apply the "state of the art" in any case. Thus, as far as Art. 25 and 32 GDPR apply, there is no higher level of protection that could be signaled by a data protection certification mechanism. As explained, Art. 25 and 32 GDPR require data controllers (and in part, processors) to take, among other aspects, the "state of the art" into account when implementing the principles listed under Art. 5 GDPR into the processing. This requirement deprives "normal" regulation addressees who develop the "state of the art" regarding a specific risk of their opportunity to refinance their development costs because they cannot use their "better" product as a unique selling point anymore. Only entities that see the development of the "state of the art" as their core business value proposition can economically benefit from this requirement. They can use the requirement as an ever-renewing business opportunity: Each time they push the "state of the art", they put the other regulation addressees under pressure to implement (and buy) these newly developed protection measures.[72] Only these entities, therefore, will have an interest in signalling the higher level of protection of their new technical or organisational solution. However, in this regard, all data protection certification mechanisms must, or at least, should refer to the constantly evolving "state of the art", and consequently, signal it. Because if they did not refer to the "state of the art", they would not be able to demonstrate that the certified processing operation complies with the "state of the art"-requirement under Art. 25 and 32 GDPR.[73] As far as Art. 25 and 32 GDPR apply, all certification mechanisms can thus not signal a higher level of protection. Therefore, different levels of protection and their respective competitive advantages are only possible, in principle, outside the scope of Art. 25 and 32 GDPR. [74]

4.2.3 Suitable objects of data protection certification mechanisms

Another question that should be clarified refers to the object of data protection certification mechanisms, that is, asking what can or should be certified. This question arises given the divergent wording used within the law. On the one hand, Art. 42 sect. 1 sent. 1 GDPR refers to "the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of *demonstrating compliance with this Regulation of processing operations* [emphasis added] by controllers and processors." On the other hand, recital 100 GDPR

[72] See above point "The 'state of the art' as a driver of market innovation (macroeconomic level)".
[73] See this consideration, in more detail, below under point "Monitoring of the 'state of the art' by certification bodies (or DPA)".
[74] This consideration applies "in principle" because the data controllers and processors do not only have to take the "state of the art" into account but also the costs of the implementation. This means that there may be a more protective solution on the market that the regulation addressees do not have to implement because its implementation costs are too high. Nevertheless, even in such a situation, the data controllers and processors could implement such a solution (even if they are not required to do so by law) and then signal this (deliberately offered) higher level of protection on the market utilising a data protection certification mechanism.

highlights the function of data protection certification mechanisms "allowing data subjects to quickly assess *the level of data protection of relevant products and services* [emphasis added]".

Some authors advocate to stick with the original wording used within the law itself, so that the wording of recital 100, which has only the function of an element for the interpretation of the law, is given little weight. von Braunmühl justifies this statement on the grounds, for example, that the certification of "something" that complies with data protection laws can logically be related only to processing operations and not to products or services. The simple reason for this is that the material scope of data protection refers to the "processing of personal data" and not to products or services.[75] Instead, other authors want that also products and services should be certifiable. These authors argue that consumers are able to understand which product and/or service has which kind of "data protection quality" better when certifying the product or service as a whole. Similarly, the marketing of data-driven products and services of high "data protection quality" can be more effective if the entire product or service is certified.[76]

Taking into account the above-described signalling function of certificates, the crucial aspect for a solution to this discussion is that certificates must not mislead consumers and/or business customers. Therefore, it is indeed correct to primarily refer to a specific "processing operation" rather than a product or service that may rely on a whole system of processing operations.[77] A data protection certification mechanism must make it clear from the perspective of the data subjects and/or the business customer, whether this is a data controller or processor, to what exactly it refers to: Is it a single processing or a whole system of operations that could involve multiple data controllers and/or processors? In the end, an answer to this question also depends on the legal provision to which the data protection certification mechanism relates: If a data controller (or processor) can use such a mechanism in order to demonstrate compliance, for instance, with the data protection and security-by-design requirements under Art. 25 and 32 GDPR, the mechanism must make it clear what is actually considered to be compliant with the specific requirement.[78] A certification mechanism must, therefore, clarify, in essence, (1) to which processing operation(s) it refers, (2) which risk this causes (that is, the likelihood and severity of the risk for the rights and freedoms of the data subjects) and (3) the implemented safeguards mitigating this risk. This means that a data protection certification mechanism can only refer to a product or service as a whole if the certification procedure addresses at least all processing operations on that the product or

---

[75] See Patrick von Braunmühl, Art. 42 Rn. 7, in: Kai Uwe Plath, BDSG/DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, (Otto Schmidt, 2nd ed., 2016).

[76] See Philip Laue, Judith Nink, Sascha Kremer, 264, Das neue Datenschutzrecht in der betrieblichen Praxis (Nomos, 1st ed., 2016); von Braunmühl, ibid.

[77] Cf. ENISA, ibid., pp. 15, 22.

[78] Cf. above under point "Degree of granularity of codes of conduct and data protection certification mechanisms"; cf. also the idea that the data protection certification mechanisms "could reward the privacy-aware technologies and offer a competitive advantage to these technologies on the single market", at Eric Lachaud, Why the certification process defined in the General Data Protection Regulation cannot be successful, 823, in: Computer Law and Security Review, 32 (6), 814–826 (2016), which would not be possible if it was unclear what kind of technology is actually used by the certified data controller or processor.

service relies on. If a certificate addresses only certain parts of the processing operations on which a product or service relies on, it must clarify these limitations.

This leads us to the main challenge that data protection certification mechanisms have to cope with. This challenge refers to the question of how such a certification mechanism should be designed so that data subjects are definitely able "to *quickly assess the level of data protection* of relevant products and services [emphasis added]."[79] A data protection certification mechanism must keep its promises. Conversely, if a data protection certification mechanism signals a different level of protection that is actually not present in that situation, this can lead to significant legal consequences: a data controller or processor may lose its certification (Art. 42 sect. 7 sent. 2 GDPR) or is subjected to another sanction mechanism (Art. 43 sect. 2 lit. d and e GDPR).[80] Moreover, this could happen because the certification body loses its accreditation (Art. 43 sect. 7 GDPR) or one or all of them receive a penalty or fine (Art. 83 sect. 4 lit. a and b GDPR).[81] The reason for these consequences could be that (1) the certification mechanism signals to cover more processing operations than it actually does, or (2) signals a lower or even another risk caused by the data processing or (3) signals more protection provided for by certain safeguards against a certain risk, but these do not work properly. In conclusion, the question of what a certification mechanism de facto signals depends on two aspects: On the one hand, an exact definition of the data processing and the level of data protection that the certification mechanism really covers. On the other hand, the specific way how both aspects (i.e. the processing and level of protection that is covered by the certification mechanism) is shown to data subjects so that they can actually understand it. While the first question may be answered by legal and technical experts, the second question may primarily be answered by user experience design. Such a combination of different disciplinary concepts makes it so difficult for the regulation addressees to meet the regulatory expectations.

4.3 Coping with complexity

The preceding considerations have shown how complex questions surrounding data protection certification mechanisms can become. This last section focuses on three particular aspects of the complexity taking the viewpoint of the following three stakeholders into account: Entities that issue data protection certification mechanisms, which means, certification bodies or data protection authorities (in the following also "DPA"); data controllers and processors wishing to submit their data processing operations(s) to a certification mechanism; and data subjects who wish to estimate the level of protection of a certain processing operations (or products and/or services) by referring to a certain data protection certification mechanism.

[79] See recital 100 GDPR.
[80] See Stefan Heilmann, Wolfgang Schulz, ibid., Art. 42, cip. 39.
[81] The sending of false signals might also conflict with the prohibition of unfair commercial practices, for example, because it is misleading, pursuant to Art. 5-7 of Directive 2005/29/EC ("Unfair Commercial Practices Directive"), Gerald Spindler considers, at least, that the German Unfair Competition Act can be principally applicable if a competitor infringes the GDPR, see Gerald Spindler, ibid.

4.3.1 The monitoring of the "state of the art" by certification bodies (or DPAs)

The first aspect to be discussed refers to the aforementioned interplay between data protection certification mechanisms and the "state of the art"-requirement under Art. 25 and 32 GDPR. As already emphasised before, all data protection certification mechanisms must or at least should refer to the constantly evolving "state of the art", as otherwise, they could not be used to demonstrate that the certified processing operation complies with Art. 25 and/or 32 GDPR.

On the one hand, this does not mean that Art. 42 and 43 GDPR *require* the certification body or DPA to constantly monitor the "state of the art". Sect. 5 sent. 1 of Art. 42 GDPR merely states that a "certification pursuant to this Article shall be issued by the certification bodies (...) or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority" or by the European Data Protection Board. Correspondingly, sect. 7 sent. 2 requires a certificate to "be withdrawn, as applicable, by the certification bodies (...) or by the competent supervisory authority where the requirements for the certification are not or are no longer met". Thus, the obligation of the certification body or the DPA depends on the approved criteria: As long as the criteria do not refer to the "state of the art"-requirement, the certification body (or DPA) does not have to assess, not even in the moment it issues the certificate, seal or mark, whether or not the data controller (or processor), who wants its data processing operation(s) to be certified, takes, sufficiently, the "state of the art" into account. Similarly, as long as the criteria only require the data controller (or processor) to apply the "state of the art" at the time the certificate is issued (but not longer), the certification body (or DPA) does not have to constantly monitor the evolvement of the "state of the art" and assess whether the data controller (or processor) still takes the "state of the art" sufficiently into account, even after the certificate was issued.

On the other hand, such a limited scope of a certification mechanism is in some way contrary at least to Art. 25 GDPR, according to which the data controller has to comply with this provision "both at the time of the determination of the means for processing and at the time of the processing itself". In summary, therefore, it must be said that the certification mechanism loses, at least, its legal certainty increasing function, the more time has passed since the certificate was issued. In contrast, if a certification body (or data protection authority) wishes to offer a data protection certification mechanism that demonstrates compliance with the state of the art-requirement throughout the period in which the mechanism is used by a controller, this body must constantly monitor the "state of the art" (and assess whether the controller applies the criteria or not). This task could become very complex if the market for technical and organisation data protection measures becomes dynamic. However, a certification body (or DPA) can perform this task much better than the typical data controller because the existence of data protection law (and its complexity) is, so to speak, the reason for its existence.

4.3.2 Modularising the scope of data protection certification mechanisms

However, even if data controllers (and processors) can outsource the monitoring of the "state of the art" to a certification body (or DPA), the procedure itself for receiving a data protection

certificate, seal or mark can still be quite complex. This may cause a conflict with Art. 42 sect. 1 sent. 2 GDPR, which states that "[T]he specific needs of micro, small and medium-sized enterprises shall be taken into account." The idea behind this provision is to organise the procedures related to a data protection certification mechanism in a way that makes it also affordable for micro-, small-, and medium-sized enterprises given their limited resources.[82] Therefore, the question arises how such procedures may be organised so that it does not divert too many "scarce resources of potentially high-growth entrepreneurial firms away from their core business."[83]

To prevent such a situation, there are two main factors: the rigour of control mechanisms and the scope of the certificate. With respect to the first factor, the certification procedure becomes more complex the more stringent the certification body (or DPA) assesses whether the data controller or processor wishing to have their data processing operation(s) certified meets the certification criteria. In this regard, Art. 42 sect. 6 GDPR states that the controller or processor must provide the certification body or DPA "with all information and access to its processing activities which are necessary to conduct the certification procedure". As such, it makes sense to adapt the depth of the assessment to the data protection risk that is typically caused by the processing operation in question.[84] However, this paper does not does not go into this question any further. In contrast, the following paragraphs will focus on the second factor, that is, the scope of the data protection certification mechanism.

As mentioned earlier, the scope of a data protection certification mechanisms depends essentially on the following aspects: First, if the certification mechanism covers only one single, several or all processing operations on which a product or service is build; second, if it covers all or only specific risks caused by such (a) processing operation(s). In this context, the risk-based approach again plays an important role.[85] Using the example of the German IT-Grundschutz model (that was developed and) is currently being modernised by the German Office for Information Security ("Bundesamt für Informationssicherheit"; in the following also "BSI"), a data protection certification mechanism could be designed in such a way that it differentiates between context-specific risks. With respect to data protection risks, a certification mechanism could thus enable controllers and processors to first concentrate on the most relevant data protection risks (caused by one or several processing operations). Subsequently, they can then extend the scope and/or gradually increase the protection level.[86]

Such a risk-based, modular data protection certification mechanism requires a robust risk assessment methodology.[87] However, regardless of how such a robust methodology should

---

[82] See Philip Laue, Judith Nink, Sascha Kremer, ibid., 263 seq., referring to the European Parliament's draft of GDPR; see also Eric Lachaud, ibid., p. 820, who emphasis the potentially discriminatory effect in detriment of companies who cannot afford the costs for going through a certification process.

[83] See above under point "Reducing the complexity of an entrepreneurial process (microeconomic level)", quoting Levie and Autio, ibid., p. 1411.

[84] Cf. Stefan Heilmann, Wolfgang Schulz, ibid., Art. 41, cip. 21, with respect to codes of conduct.

[85] See, in particular, Art. 24, 25 and 32 GDPR; Stefan Heilmann, Wolfgang Schulz, ibid., Art. 42, cip. 35.

[86] See Bundesamt für Informationssicherheit, Motivation und Ziele der Modernisierung des IT-Grundschutzes, available under. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/Motivation/itgrundschutz_motivation_node.html, (re-called the 3 October 2017).

[87] Cf. Raphael Gellert, ibid. pp. 490-492.

be designed, the following examples are intended to illustrate how such a modular scheme could look like: for example, a module of such a certification mechanism could guarantee a certain level of protection for how personal data is pseudonymised. This could be important information that a data controller would like to signal to data subjects if its processing activities do not require to identify them. If the risk of re-identification is the most relevant in this context, the controller may focus on submitting its processing operation(s) to only one certification mechanism that exclusively covers this risk, even if there are, in principle, more risks caused by the processing. In a second step, the controller could then focus on another risk, such as intransparent data processing, and add a module of the certification mechanism that specifically covers this additional risk. This module may ensure that the controller implements a system of specially designed pictograms that intuitively clarify the content of the information provided to the data subjects. In summary, it depends on an assessment of the most relevant risk caused by the processing activities and the strategy regarding the controller's (or processor's) position in the market, which processing operation and which risk is first certified, which part comes next and so on. Such a modular data protection certification mechanism could at least reduce the efforts significantly when undergoing a certification process, significantly.

On the other hand, a modular certification mechanism that enables data controllers and processors to differentiate not only between processing operations but also between the risks that a processing operation can cause, further increases the complexity for the data subject.[88] To avoid the situation where a data subject does not understand what type of risk was caused, for example, by a bundle of processing operations on which a data-driven product is build on, the data protection certification mechanism must clearly signal its scope. Here again, it will be a question for future research how such a modular scheme has to be worked out in order to not deceive the data subjects. This question may specifically address the domain of user experience design. Another question is, in fact, whether it is (both technically and normatively) possible to separate different risks from each other. It may well be the case that one risk is extremely related to another so it cannot be mitigated separately. In such a case, it would probably be misleading for the data subject if a data protection certification mechanism relates to only one of the two risks. In that case, such a data protection certification mechanism had thus to relate to both risks and the corresponding level of protection.

4.3.3 The degree of diversity of certificates offered on the market

From the point of view of data subjects, the complexity increases further if one takes into account that there is not only one certification body operating on the "data protection market" but in principle an unlimited number of them. This can lead to the situation where data subjects (completely) loose the overview.[89] Then these mechanisms lose their function to effectively signal the level of protection of, let us say, a data-driven product that operates on

[88] See already above point "Suitable objects of data protection mechanisms".

[89] See ENISA, ibid., p. 24; Rowena Rodrigues, David Barnard-Wills, Paul De Hert & Vagelis Papakonstantinou, ibid., p. 257.

the basis of a bundle of processing operations to a data subject who wishes to purchase that product.[90]

A solution to such market fragmentation is, of course, to centralise the offer. If fewer entities offer certificates on a "data protection market", there is a smaller risk of the market to become too fragmented. For example, if only data protection authorities were allowed to offer data protection certification mechanisms,[91] the number of certification bodies in the European Single Market would (almost) equal the number of EU Member States.[92] One can also categorise the European Data Protection Seal as a similar mechanism, which may even add to the previous mechanism. Pursuant to Art. 42 sect. 5 GDPR, as mentioned before, a certification can only be issued by a certification body or a DPA on the basis of criteria approved by that DPA or the European Data Protection Board; if the European Data Protection Board approves the criteria, sent. 2 regulates that "this may result in a common certification, the European Data Protection Seal." If this certification mechanism is established in a way that includes all other corresponding national mechanisms that could be operated by private certification bodies or DPAs, it will have a resounding, harmonising, even homogenising effect on the "data protection market".[93]

As already explained, however, such a solution based on the centralisation of knowledge may conflict with the need for market creativity. Such market creativity is at least necessary when a central entity is unable to react quickly enough to the dynamics of innovative markets, which essentially means to collect the necessary knowledge about context-specific risks and the corresponding measures that can best mitigate those risks.[94] From this perspective it can be better to allow a multitude of entities to act as certification bodies so that they can create a variety of data protection certification mechanisms that can cover the variety of context-specific risks. On the one hand, such a homogenising, in other words, "creativity-reducing" effect does not seem to be severe if a European Data Protection Seal addresses only specific data protection risks caused by certain processing operations.[95] In this case, the market can still develop its creative dynamics by discovering new processing operations or new risks (which do not necessarily have to be caused by new operations but may also be caused by already well known operations), and thus quickly find suitable solutions. Only if a European Data Protection Seal covered a wide range of processing operations and risks —providing for

[90] See above under point "Signalling a certain level of protection to market participants (mesoeconomic level)", referring to Wegner, ibid., pp. 80-82.

[91] However, see the risks of such a solution discussed at Rowena Rodrigues, David Barnard-Wills, Paul De Hert, Vagelis Papakonstantinou, ibid., pp. 262-263; see also ENISA, ibid., p. 25.

[92] However, in Germany, the market may remain rather fragmented in light of its federal structure, which leads to more than 16 data protection authorities, cf. Peter Schaar, Datenschutz und Föderalismus. Schöpferische Vielfalt oder Chaos, cip. 36-37, in: Ines Härtel, Handbuch des Föderalismus - Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt. Band III - Entfaltungsbereiche des Föderalismus (Springer, 1st ed., 2012).

[93] Cf. Rowena Rodrigues, David Barnard-Wills, Paul De Hert, Vagelis Papakonstantinou, ibid., p. 264, discussing the opposite constellation, that is, the negative effects, if there were a European privacy Seal that does not include any other seals operated by the DPA.

[94] See above under point "Openness of regulatory instruments to innovation".

[95] Cf. the considerations above point "Level of protection signaled by data protection certification mechanisms" and "Suitable objects of data protection certification mechanisms".

criteria on a rather abstract level – this would hamper the required market creativity. In this case, however, the criteria may not adequately specify the law, but functions at a similar abstract level such as the law itself.[96]

Besides the simple reduction of the certification mechanism, however, there are also "softer" solutions.[97] Among them, a solution should be discussed quickly, as it addresses, in particular, the problem that data subjects may be unable to keep track of all the variety of certificates. DPAs could help data subjects to obtain and/or maintain an overview about certificates that best meet their specific needs by testing and ranking the quality of data protection certification mechanisms. In this case, DPAs do not only act as entities supervising the creation and control of the data protection certification mechanisms by private certification bodies, which are subject to their competencies. They can also compare data protection certification mechanisms across the European market.[98] In this regard, the registration and publication of data protection certification mechanisms in the European Single Market, pursuant to Art. 42 sect. 8 GDPR, is an important step. In order to enable such a European-wide comparison, this provision should therefore be understood in a way that not only European Data Protection Seals have to be registered, but also national data protection certification mechanisms.[99] Through publicity the regulator can also learn which mechanisms work best in which context under which conditions, and frequently (re-)evaluate and (re-)adapt its regulatory instruments according to its regulatory objectives.[100]

Only if the regulator, for example, the European Data Protection Board concludes that these "creativity-preserving" mechanisms do not give the data subjects the necessary overview, it should consider further steps, such as reducing the number of data protection certification mechanisms.

5. Conclusion

The preceding considerations addressed the question under which conditions the political promise that the GDPR gives its regulation addressees of a competitive advantage could apply in business practice. Integrating concepts of evolutionary market theories and entrepreneurship

[96] Cf., for example, the "EuroPriSe Criteria for the certification of IT products and IT-based services", which do not make further differences between IT products and services, https://www.european-privacy-seal.eu/EPS-en/Criteria (3 March 2018); in contrast, see the considerations regarding the ISO Cloud Standard at Paul de Hert, Vagelis Papakonstantinou, Irene Kamar, ibid., p. 27, which seems therefore to be a better example.

[97] See, for example, Rowena Rodrigues, David Barnard-Wills, Paul De Hert, Vagelis Papakonstantinou ibid., pp. 256 subseq., focusing on the available options of the European Commission to enhance the implementation of data protection certification mechanisms.

[98] Consumer protection agencies could take over such a function, as well, as long as the data-driven service being certified creates the overlap between data protection and consumer protection law, in other words, in situations where data subjects are, simultaneously, consumers; cf., regarding the variety of questions on the interplay between data protection law, consumer protection law, and competition law, Preliminary Opinion of the European Data Protection Supervisor (EDPS), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, 26 (March 2014).

[99] Leaving open that question, ENISA, ibid., p. 27.

[100] Cf. Martin Eifert, ibid., cip. 60; Claudius Franzius, ibid., cip. 81-103.

research to the equation, the regulator is, at least in principle, able to strengthen competition in the "data protection market(s)". In this regard, legal principles and broad legal terms such as the data protection and security-by-design requirements, combined with co-regulatory instruments, in particular, the data protection certification mechanisms and codes of conduct, can play a major role. The reason for this is that in innovative and dynamic environments, the regulator is hardly able to centralize the knowledge about context-specific risks and thus the necessary protection instruments. Legal principles and broad legal terms can therefore be appropriate regulatory instruments because they leave the regulation addresses enough room to explore, in accordance to their specific context, the risks and thus the best solution to mitigate these risks. By using codes of conduct, and even more so, data protection certification mechanisms, data controllers and processors can turn the vagueness of the law into a competitive advantage. These effects can be demonstrated on three different levels:

At the microeconomic level, data controllers and partly processors, are able to increase legal certainty by specifying and standardising legal principles and broad legal terms through these co-regulatory instruments. The increase in legal certainty offers them a competitive advantage because it reduces the complexity of their entrepreneurial process. This function is inherent in both instruments, that are, codes of conduct and data protection certification mechanisms (and BCR, to a very limited extent). However, the previous analysis has shown that both instruments increase legal certainty, the more detailed they specify the law; if they merely repeat the wording of the law, their function in increasing legal certainty is zero. The incentive of data controllers and processors to use these legal instruments varies depending on what they lose or gain when they can demonstrate compliance with the law or, vice versa when it turns out that they violate the law. The higher the investments or the expected profits are, the more likely it is that they want to make sure that they are legally compliant. The question of how these positive and negative incentives (gaining trust of consumers or business customers versus receiving a fine) should be designed to make sure that the potential of the legal certainty increasing function is fully exploited, must also be researched empirically.

In contrast to codes of conduct, data protection certification mechanisms can also offer, at least in principle, a competitive advantage on a mesoeconomic level. The reason for this is that controllers and processors can: first, use the vagueness of legal requirements as a business opportunity to offer their consumers or business customers a higher level of protection than their competitors do (so that their customers and/or consumers pay a higher price or buy more products of this higher quality). Whether the GDPR allows such a competitive function or only aims for the compliance function (that is, to reduce legal certainty) is debated in legal literature. Regardless of the outcome of this debate, the previous analysis has shown that there are only a few cases where such a competitive function could become relevant. Firstly, the question becomes only relevant if there is (1) a specific processing operation with (2) a specifically defined risk and (3) different safeguards lead, in fact, either to a higher or lower level of protection. Given the multitude of processing operations and different risk (whether the risks are truly different or just higher or lower) most data protection certification mechanisms do not signal a higher or lower level of protection but simply refer to another (incomparable) case. Secondly, even if two (or more) specific processing operations create the same risk and

thus safeguards could provide a higher or lower level of protection (which could be signalled by a data protection certification mechanism), there is another legal mechanism that limits the potential competitive advantage of this situation. This legal mechanism is the "state of the art"-requirement under Art. 25 and 32 GDPR, which obliges data controllers, and in some cases processors, to constantly be on the same page as the new, higher level of protection offered on the market (or to at least "take it into account"). Therefore, there is only a small room for manoeuvre in which different levels of protection become relevant. Such a limitation on the variety of data protection certification mechanisms on the market might not be the worst result, as it is already difficult enough to signal a specific level of protection of a specific processing operation to the data subject, so that they understand it correctly. How this, in the end, should be done cannot only be answered by legal and technical expertise but additionally, through means of user experience design.

The "state of the art"-requirement under Art. 25 and 32 GDPR is another factor that can boost innovation even at the macroeconomic level. This requirement can enhance innovation if specialised companies focus on developing the "state of the art" and put it as their core value proposition for the other "normal" regulation addressees. These specialised entities can use the requirement as a business opportunity that constantly renews itself because they constantly put pressure on other regulatory addressees to implement (and buy) the "state of the art", which they themselves are pushing ahead time and again. If this mechanism creates a dynamic market for data protection-by-design solutions, it can get quite difficult for data controllers and processors to see what the "state of the art" of a solution against a specific risk caused by a certain data processing operation currently is. In this regard, certification bodies (and DPA) can play an important role. If a certification mechanism offered by these bodies has to prove, pursuant to its criteria, compliance with the "state of the art"-requirement, and possibly not only in the moment the certificate, seal or mark is issued but also throughout the period when it is in use, the certification body has to constantly monitor the market for the "state of the art" and frequently re-assess whether the data controller still complies with it or not. Such a function of data protection certification mechanisms can be an important benefit and thus an incentive for data controllers to use these certification mechanisms because it significantly reduces the complexity to comply with the law.

However, this does not mean that the process through which data controllers and processors must go through to certify one or more of its processing operations is not complex. The legislator has clearly seen that the complexity of certification mechanisms can conflict with the needs of micro-, small- and medium-sized companies due to their limited resources. One way to reduce this complexity is to limit the scope of a data protection certification mechanism, in addition to financial aids or reducing the depth of how compliance with the criteria of such a mechanism is controlled. For example, if a data controller can choose a certification mechanism that addresses only a specific risk for a particular processing operation of which the controller thinks that its level of protection is most relevant to be signaled on the market, the procedural complexity is limited to this particular case. In contrast, the procedural complexity increases the more data processing operations and the more risks the certification mechanism aims to cover. To find a balance between scaling the mechanisms and reducing its

complexity, the mechanisms could be modularised so that data controllers and processors could begin with one module that covers a specific risk of a particular operation, adding more modules step by step, expanding to further risks and further operations. How such a modularised mechanism must be designed so that data subjects can truly understand which risk of which processing operation the specified module of the data protection certification mechanism covers depends not only on legal and technical expertise but also on research in the field of user experience design.

Finally, from the point of view of data subjects, the degree of complexity of data protection certification mechanisms is also relevant. The previous considerations have shown that the market success of such mechanisms depends on whether data subjects can actually understand which mechanism signals which level of protection for which processing operation. For the data subjects, this is an already very complex issue, which is all the more valid the more certification mechanisms are offered on the market. One solution to reducing this complexity is to reduce the number of certification mechanisms. In this respect, the European Data Protection Seal can be crucial, given that this mechanism harmonises the criteria according to which national certification mechanisms are issued to data controllers and processors. However, this mechanism should not lead to the the situation in which the market creativity loses its ability to react quickly and effectively to newly discovered risks or even unknown operations. This situation can be avoided if European Data Protection Seals are sufficiently specific, that is, are not based on abstract-general criteria, but refer to specific risks of certain processing operations. This indeed poses the same questions as before.

After all, these are just a few of the remaining questions; and even these few questions show that research into the impact of regulatory instruments on data-driven innovation and competitive advantage is a rather complex issue. The complexity requires the ability of a regulator to learn, and thus to frequently (re-)evaluate and (re-)adapt its regulatory instruments according to its goals.[101] If done well, this approach will at least increase the rationality of the law, regardless of whether or not the political promise that the GDPR provides for competitive advantage becomes true.[102]

[101] Cf. Martin Eifert, ibid., cip. 60; Claudio Franzius, ibid.,, cip. 81-103.
[102] Cf. Hoffmann-Riem, Saskia Fritzsche, ibid., p. 39.

Literature

Alvarez, Sharon; Barney, Jay B.	Discovery and Creation: Alternative Theories of Entrepreneurial Action, in: Strategic Entrepreneurship Journal 1 (1) 11-26 (2007)
Appelt, Ivo	Aufgaben und Verfahren der Innovationsfolgenabschätzung (Tasks and Procedures of the Innovation Impact Assessment), in: Martin Eifert, Wolfgang Hoffmann-Riem, Innovation und Recht III – Innovationsverantwortung, 147–181 (Mohr Siebeck, 1st ed., 2009)
Article 29 Data Protection Working Party	Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP 218, available under: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf, (30 May 2014)
Id.	Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, available under: ec.europa.eu/newsroom/document.cfm?doc_id=47711, (4 April 2017)
Baldwin, Robert; Cave, Martin; Lodge, Martin	Understanding Regulation – Theory, Strategy and Practice, (Oxford Press, 2nd ed., 2013)
Baumgartner, Ulrich; Gausling, Tina	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, in: ZD 2017, 308.
Bennett, Colin J.; Raab, Charles D.	Colin J. Bennett, Charles D. Raab 'The Governance of Privacy: Policy Instruments in Global Perspective', (MIT Press, updated paperback ed., 2006)
Bergt, Matthias	Art. 42 cip. 15, in: Jürgen Kühling, Benedikt Buchner, Datenschutz-Grundverordnung - Bundesdatenschutzgesetz (CH. Beck, 2nd ed., 2018)
Black, Julia	Forms and Paradoxes of Principles Based Regulation, in: Capital Markets Law Journal, 3 (4), 425-457, (2008)
Blind, Knut	The Impact of Standardization and Standards on Innovation., in: Manchester Institute of Innovation Research (ed.), Compendium of Evidence on the Effectiveness of Innovation Policy Intervention, (2013), availabe under: <http://www.innovation-policy.org.uk/compendium/section/Default.aspx?topicid=30.>
Borraz, Olivier	Les politiques du risque (Presses de Sciences Po, 1st ed., 2008)
von Braunmühl, Patrick	Art. 42, in : Kai Uwe Plath, BDSG/DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, (Otto Schmidt, 2nd ed., 2016).
Bundesamt für Informationssicherheit (BfS)	Motivation und Ziele der Modernisierung des IT-Grundschutzes, available under. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/Motivation/itgrundschutz_motivation_node.html, (re-called the 3 October 2017).
Bygrave, Lee A.	Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements., in: Oslo Law Review, 4 (2), 105-120, (2017)
Costa, Luiz	Privacy and the precautionary principle, in: Computer Law & Security Review,

28 (1), 14-24, (2012).

Eifert, Martin — Regulierungsstrategien (Regulation Strategies), in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012)

EU Agency for Network and Information Security — ENISA, Recommendations on European Data Protection Certification, Version 1.0, 13, (November 2017)

European Data Protection Supervisor (EDPS) — Preliminary Opinion of the European Data Protection Supervisor (EDPS), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, (March 2014).

Evers, Adalbert; Nowotny, Helga — Umgang mit Unsicherheit (Suhrkamp, 1st ed., 1987)

Fagerberg, Jan — Innovation: A Guide to the Literature, „What innovation is not: the linear model", in: Jan Fagerberg, David C. Mowery (eds.), The Oxford Handbook of Innovation (Oxford University Press, 1st ed., 2004)

Franzius, Claudio — Modalitäten und Wirkungsfaktoren der Steuerung durch Recht (Modes and Impact Factors for the Control through Law), § 4, in: Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle (eds.), Grundlagen des Verwaltungsrechts – Band I „Methoden – Maßstäbe – Aufgaben – Organisation", (C.H. Beck, 2nd ed., 2012)

Friedewald, Michael; et. al. — Forum Privatheit, White Paper Datenschutz-Folgenabschätzung., available under: http://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf, (2017)

Gartner, William B. — A Conceptual Framework for Describing the Phenomenon of New Venture Creation, in: The Academy of Management Review 10 (4) 696-706 (1985)

Gasser, Urs — Cloud Innovation and the Law: Issues, Approaches, and Interplay, No. 2014-7 19-20, available under : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410271

Gawel, Erik — Technologieförderung durch „Stand der Technik": Bilanz und Perspektiven, in: Martin Eifert, Wolfgang Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 197-220, (Duncker & Humblot, 1st ed. 2009)

Gellert, Raphael — Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative, in: International Data Privacy Law, 5 (1), 3-19, (2015)

Gellert, Raphael — We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection, in: European Data Protection Law Review (EDPL), 4 (2), 481-292, (2016)

v. Grafenstein, Max — The Principle of Purpose Limitation in Data Protection Laws: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation, (Mohr Siebeck, 1st ed., 2018, to be published)

de Hert, Paul; Papakonstantinou, Vagelis; Kamara, Irene — The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection, in: Computer Law & Security Review, 32 (1), 16-30, (2016)

Hartog, Chantal et. — Institutions and Entrepreneurship: The Role of the Rule of Law, 8. (7 January 2018), available under: http://ondernemerschap.panteia.nl/main/publication/bestelnummer/h201003

Hirsch, Dennis D. — In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct, in: Ohio St. LJ, 74 (6), 1029 subseq., (2013)

Hoffmann-Riem, Wolfgang — Innovationsoffenheit und Innovationsverantwortung durch Recht – Aufgaben rechtswissenschaftlicher Innovationsforschung (Openness toward Innovation and Responsibility for Innovation by means of Law), in: Archiv des öffentlichen Rechts 123 (4) 513–540 (1998)

Hoffmann-Riem, Wolfgang; Fritzsche, Saskia — Innovationsverantwortung - Zur Einleitung, 39, in: Martin Eifert, Wolfgang Hoffmann Riem (eds.), Innovations und Recht III - Innovationsverantwortung, 11-41, (Duncker & Humblot, 1st ed., 2009)

Hornung Gerrit; Hartl, Korbinian — Datenschutz durch Marktanreize - auch in Europa? (Data Protection through Market Incentives – in Europe, too?), in: ZD 4 (5) 219-225 (2014) .

Jaeckel, Liv — Gefahrenabwehrrecht und Risikodogmatik – Moderne Technologien im Spiegel des Verwaltungsrechts (Prevention of Danger through Law and Legal Conceptualization of Risk), 51- 52, (Mohr Siebeck, 1st ed., 2010)

Jarass, Hans D. — Bundes-Immissionsschutzgesetz, BImSchG (C.H. Beck, 12th ed., 2017)

Jergl, Johann — Art. 32, cip. 21 subseq.., in: Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel, Winfried Veil, Kommentar Datenschutz-Grundverordnung,, (Bundesanzeiger Verlag, 1st ed, 2017)

Kamara, Irene — Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate, in European Journal of Law and Technology, 8 (1), 8-11, (2017)

Kaplow, Louis — Rules Versus Standards: An Economic Analysis, in: Duke L. J., 42 (3), (1992)

Kloepfer, Michael — Law enables Technology – About an underestimated function of environmental and technology law, in: Natur und Recht 417–418 (1997).

Kroes, Neelie — Statement by Vice President Neelie Kroes ,on the consequences of living in an age of total information´ from the 4th of July 2013, (Sep. 30, 2017), available under: http://europa.eu/rapid/press-release_MEMO-13-654_en.htm

Lachaud, Eric — Why the certification process defined in the General Data Protection Regulation cannot be successful, 820, in: Computer Law and Security Review, 32 (6), 814–826 (2016)

Lachaud, Eric — The General Data Protection Regulation and the rise of certification as a regulatory instrument, in: Computer Law and Security Review (March 2017)

Laue, Philip; Nink, Sascha — Das neue Datenschutzrecht in der betrieblichen Praxis (Nomos, 1st ed., 2016)

Levie, Jonathan; Autio Erko	Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, 1411. in: Journal of Management Studies 48 (6) 1392–1419 (2011)
Martini, Mario	Integrierte Regelungsansätze im Immissionsschutzrecht, (C.H. Beck, 1st ed., 2000)
Maxwell, Winston J.	Principles-based regulation of personal data: the case of ‚fair processing, in: International Data Privacy Law, 5 (3), 205-216, (2015)
Mayer-Schönberger, Viktor	Mayer-Schönberger, The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship, 6 (2) 159-169 (2010)
Moser, Jana	Art. 25, cip. 59 subseq.;Art. 32, cip. 21 ff., in: Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel, Winfried Veil, Kommentar Datenschutz-Grundverordnung,, (Bundesanzeiger Verlag, 1st ed, 2017)
Murray, Andrew	Conceptualising the Post-Regulatory (Cyber)state, in: Roger Brownsword, Karen Yeung (eds.), ibid., 287–316 (2008)
Murray, Andrew	The Regulation of Cyberspace – Control in the Online Environment In: Modern Law Review 70, (5) 879–883 (2007)
Paal, Boris B.; Pauly, Daniel A.	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, DS-GVO - BDSG, (C.H. Beck, 2nd ed., 2018)
Peel, Jacqueline	Science and Risk Regulation in International Law, (Cambridge University Press, 1st ed., 2010).
Peretti-Watel, Patrick	La société du risque (Repères. La Découverte, 1st ed., 2010)
Posner, Richard A.	Economic Analysis of Law, (Aspen/Wolters, 8th ed., 2010).
Rodrigues, Rowena; Barnard-Willsa, David, De Hert, Paul; Papakonstantinou, Vagelis	The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR, 249, in: International Review of Law, Computers & Technology, 30 (3), 248–270, (2016), available under: <http://dx.doi.org/10.1080/13600869.2016.1189737>
Roßnagel, Alexander	Roßnagel, Data protection in computerized everyday life, (2007), Gutachten im Auftrag der Friedrich-Ebert-Stiftung, available under: http://library.fes.de/pdf-files/stabsabteilung/04548.pdf
Raab, Charles D.; De Hert, Paul	Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood, in: Roger Brownsword, Karen Yeung (eds.), Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes, 263–285 (2008)
Rodrigues, Rowena, Wright, David, Wadhwa, Kush	Developing a privacy seal scheme (that works), in: International Data Privacy Law, 3 (2), 100-116 (2013)
Schaar, Peter	Datenschutz und Föderalismus. Schöpferische Vielfalt oder Chaos, in: Ines Härtel, Handbuch des Föderalismus - Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt. Band III - Entfaltungsbereiche des Föderalismus (Springer, 1st ed., 2012).
Schumpeter, Joseph	Capitalism, Socialism & Democracy, 82-83 (5th ed. 2003)
Spindler, Gerald	Nationale Umsetzung der Datenschutzgrundverordnung im Bereich der Ko-

Regulierung - Politikempfehlungen zur Schaffung rechtlicher Anreize für die Wirtschaft zur Entwicklung und Implementierung von Verhaltensregeln und Zertifizierungen, availabel under: https://sriw.de/images/pdf/2016-Gutachen-EU-DSGVO-SRIW---final_druck.pdf, (2016)

Steele, Jenny — Risks and Legal Theory, (Hart Publishing, 1st ed., 2004)

Tomšič, Andrej; Burnik, Jelena et al. — Consolidated report on enhancing confidence and acceptability of new certification measures., CRISP project, (2017)

Wegner, Gerhard — Nachhaltige Innovationsoffenheit dynamischer Märkte (Dynamic Markets and their Persistent Openness to Innovation), in: Martin Eifert, Wolfgang Hoffmann-Riem (eds.), Innovationsfördernde Regulierung – Innovation und Recht II, 71-91, (Duncker & Humblot, 1st ed. 2009)

Veil, Winfried — Art. 24, cip. 78-190, in: Sibylle Gierschmann, Katharina Schlender, Rainer Stentzel, Winfried Veil, Kommentar Datenschutz-Grundverordnung,, (Bundesanzeiger Verlag, 1st ed, 2017)