Jakobi, Timo et al.

The Role of IS in the Conflicting Interests Regarding GDPR

Business & Information Systems Engineering

Provided in Cooperation with:
Springer Nature

Suggested Citation: Jakobi, Timo et al. (2020) : The Role of IS in the Conflicting Interests Regarding GDPR, Business & Information Systems Engineering, ISSN 1867-0202, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 62, Iss. 3, pp. 261-272, https://doi.org/10.1007/s12599-020-00633-4

Bus Inf Syst Eng 62(3):261–272 (2020)
https://doi.org/10.1007/s12599-020-00633-4

DISCUSSION

The Role of IS in the Conflicting Interests Regarding GDPR

Timo Jakobi · Maximilian von Grafenstein · Christine Legner · Clément Labadie · Peter Mertens · Ayten Öksüz · Gunnar Stevens

Published online: 9 March 2020

1 Introduction

Timo Jakobi, Information Systems esp. IT-Security and Privacy, University of Siegen

Since May 25 2018, the General Data Protection Regulation (GDPR) regulates the handling of personal data both for companies in the European Union and European Citizens. It is part of the European Union's Digital Single Market strategy and aims to create the conditions for an economy without barriers that would benefit individuals and companies as well as society as a whole (European Parliament and Council 2016).

The protective purpose of the GDPR is to enable individuals, against the background of modern data processing possibilities and techniques and their risks, to decide for or against a consent to data processing on the basis of appropriate information on how their personal data are handled and in a self-determined manner. At the same time, the GDPR has established many fundamentally new concepts, thereby opening new leeway for legal, scientific and practical interpretation, providing both challenges and potential for renewal and innovation.

Almost two years after the entry into force of the GDPR, it seems appropriate to reflect on first effects, suggestions for improvement and future high potential research areas. With Business and Information Systems Engineering research focusing on socio-technical systems for digital data processing for commercial or social purposes, it seems that it is the natural place for a transdisciplinary examination of the possibilities and challenges that this new regulation brings along. In this regard, BISE is – maybe better than any other field – suited to address such complex questions at the intersection of law, design, organizational research and information systems. However, with evolvement of its context, maybe also the field itself needs to adapt

One sign for this simultaneous potential need and opportunity is the vivid research surrounding GDPR in the areas concerning the interdisciplinary field of BISE. In the vast majority of these contributions, a key question revolves around the interpretation of certain aspects of GDPR. On a more practical level, for example, there is an increasing body of practical guides or implementation guidelines, looking at how organizations will have to move forward to comply and avoid fines or negative publicity (Tankard 2016; Huth 2017; Voigt and Von dem Bussche

The original online version of this article was revised due to a retrospective Open Access order.

Dr. T. Jakobi (✉) · Prof. Dr. G. Stevens
Information Systems esp. IT-Security and Privacy, University of Siegen, Siegen, Germany
e-mail: timo.jakobi@uni-siegen.de

Prof. Dr. M. von Grafenstein
Berlin University of the Arts, Einstein Center Digital Future, Berlin, Germany

Prof. Dr. C. Legner · C. Labadie
Faculty of Business and Economics (HEC), University of Lausanne, Lausanne, Switzerland

Prof. Dr. Dr. hc. mult. P. Mertens
School of Business, Economics and Society and Faculty of Engineering, University of Erlangen-Nuremberg, Nuremberg, Germany

Dr. A. Öksüz
Consumer Association of North Rhine-Westphalia, Düsseldorf, North Rhine-Westphalia, Germany

2017; Lambrinoudakis 2018). However, there is a lot of criticism remaining (Cvik et al. 2018).

Organizational and management research likewise seeks to uncover and address organizational and business needs with regard to GDPR. These include, for example, the new requirements to react to data breaches (Karyda and Mitrou 2016). Researchers also try to make use of existing structures and processes such as from the information security management system (ISMS) context, to make transition for organizations easier (Lopes et al. 2019). Notably, the interpretation of a risk-based approach as used in ISMS is also present in the GDPR (Gellert 2018). But even if compliance has been reached, organizations still need support in how to communicate the measures taken effectively (Fox et al. 2018).

From a technical perspective, GDPR also imposes technical challenges in information systems design, such as the implementation of making its system "forget" (Politou et al. 2018). Moreover, the implementation and benefits of different existing technical means such as pseudonymization or anonymization must be (re-)assessed with respect to demands in GDPR (Hintze and El Emam 2018).

On the individual level, likewise, the need for interpretation is high: The newly provided rights of the data subject are being studied, e.g., from a HCI perspective (De Hert et al. 2018; Alizadeh et al. 2019). At the same time, GDPR has also given new drive to almost traditional research topics such as privacy policies as well as the issue of "informed consent" (Politou et al. 2018; Utz et al. 2019) and how to design for transparency (Jakobi et al. 2019a). Also, in absence of the ePrivacy regulation, online tracking has come to focus on the context of GDPR (Degeling et al. 2018; Ermakova et al. 2018; Schelter and Kunegis 2018; Jakobi et al. 2019b; Mhaidli et al. 2019).

The margin opened up is also noticeable with regard to law research, where GDPR was and is heavily debated (De Hert and Papakonstantinou 2016; Mitrou 2017): The new regulation must be brought in line and act in concert with existing legislation (Diker Vanberg and Ünver 2017). The role of certification mechanisms as a regulatory instrument is one major concern here (Lachaud 2018). While the aforementioned contributions stem from a certain research field or perspective, they are not only interesting, but also highly relevant for the respective other ones, because of the fact that handling the GDPR is a multi-stakeholder task by nature.

In this contribution to the ongoing discussion of the future of BISE and its relation to GDPR, we have summoned renowned experts from the fields of law, customer protection, economics, organizational and information sciences, as well as human–computer interaction to talk about how BISE research is interdependent with the GDPR in terms of contributing to an understanding of how to interpret regulation in the practice of BISE. We will particularly look at the question of which role BISE should take in the ongoing application and interpretation of GDPR. What are – before the background of its fields of expertise – meaningful, yes perhaps necessary contributions that the community can perform or must perform in the context of the GDPR? What can a research agenda therefore look like with respect to GDPR?

For contributing to an answer to these questions, we summarize the discussion initially held at the 14. Internationale Tagung Wirtschaftsinformatik (WI2019) in Siegen, Germany, supplemented with additional insights from further perspectives of academia in the field of BISE. While previous sections of this discussion section have looked at digitalization as a technological mega-trend (Legner et al. 2017; Riedl et al. 2017; Urbach et al. 2019), this time the regulatory reaction shall be discussed regarding the implications for both economy and academia, and BISE in particular. In this regard, this updated summary especially provides the multitude of perspectives necessary to cover such an interdisciplinary issue as data protection is reflected by contributions from numerous fields. All experts share the notion that data protection is an important component of a modern society, but they may differ in how to practically apply data protection regulation.

2 The EU General Data Protection Regulation Outside the Box: Competitive Advantages and Openness to Innovation

Maximilian von Grafenstein, University of Arts Berlin, Einstein Center Digital Future

Long before its application in May 2018, the EU General Data Protection Regulation (GDPR) triggered numerous controversies (De Hert and Papakonstantinou 2016). The excitement about the GDPR is based on the novel regulatory approach, which follows from the special nature of its subject matter and environment. At first glance, the GDPR may regulate the processing of personal data. At second glance, however, this law is about controlling the risks that arise for people when data that relates to them is processed (Albrecht 2016). Furthermore, recognizing the dynamics of data-driven innovation as an essential element of our digital society, all involved actors – from the legislator and data protection authorities up to data controllers, processors and data subjects – face similar knowledge uncertainties. This understanding goes hand in hand with a fundamental change in the regulatory approach of the GDPR itself and its interpretation (Zarsky 2016). Business informatics (BI) can make a significant contribution to this change.

2.1 Lawmaking and Enforcement under Knowledge Uncertainties: From a Compliance Approach to a Proactive Application of Laws

Schumpeter was one of the first economists to recognize innovation as the real driving force of social change (see the following line of arguments at von Grafenstein 2020). He saw "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 most important impulse "that sets and keeps the capitalist engine in motion" (Schumpeter 2003, pp. 82–83). A legislator who intervenes in such an evolutionary market inevitably faces the knowledge uncertainties created by its innovations. The regulation of risks and, more recently, the regulation of innovation put this kind of knowledge uncertainty into the center of their approach. While the regulation of risks addresses the question of the appropriateness of protection measures against such risks (Jaeckel 2010), the approach of innovation regulation raises the additional question of how such protection measures should be designed so that they do not unnecessarily hinder innovation or even promote it (Hoffmann-Riem 2006). Interestingly, economists deal with the phenomenon of knowledge uncertainty in an almost mirror-inverted way: The Discovery and Creation Theory, two economic approaches, both deal in particular with the knowledge certainty and uncertainty of the innovative entrepreneur, i.e. the actor who brings an innovation onto the market (Schumpeter 2003, p. 132). Both theories address the question of how entrepreneurs use business opportunities in their entrepreneurial process: Do they discover business opportunities or do they create these opportunities themselves (Alvarez and Barney 2007)? In both cases – and this is the crucial point – the law can be understood as a factor of the entrepreneurial environment (Gartner 1985), which does not have to be an obstacle to innovation, but can promote innovation if properly designed (Mayer-Schonberger 2010).

Against this background, legal principles and undetermined legal terms are much better suited for designing a law that is open to innovation than specific "command and control" rules. The reason for this is that such legal instruments give an innovative entrepreneur, as the addressee of the regulation, much more leeway to find the best solution for implementing the law in his or her specific case. At the same time, however, this approach creates considerable legal uncertainty as neither the companies nor those affected, e.g. data subjects, can know with certainty whether or not the entrepreneur's concrete implementation of the law meets the expectations of the regulator (Eifert et al. 2012). Applying these considerations to the GDPR, one recognizes immediately that this law is actually very open to innovations: it is literally peppered with legal principles and undetermined legal terms (see in particular the principles under Article 5 GDPR, for example, the purpose limitation principle, and under Article 25 GDPR, for example, the concept of risk). Here the GDPR leaves a considerable room for maneuver for the controller as well as the processors, which they can determine proactively under consideration of the characteristics of their specific case. However, this room for maneuver also leads, as already mentioned, to a considerable legal uncertainty.

2.2 Under Which Conditions Can the GDPR Offer Competitive Advantages? The Risk-Based Approach, Certificates and Codes of Conduct

In fact, no observer sees the legal uncertainty associated with the GDPR as a competitive advantage. In contrast, empirical studies demonstrate that legal uncertainty generally has negative effects on companies (Hartog et al. 2011; Levie and Autio 2011). Interestingly, even if legal certainty is high, small and medium-sized enterprises hardly profit if compliance with the law means too much expenditure for them. Due to their small size, compliance costs are quickly disproportionately high (Levie and Autio 2011). This raises the question of how a legislator can design innovation-friendly laws while keeping legal uncertainty and bureaucratic costs low. With regard to the GDPR, this is possible in three ways:

First, the so-called risk-based approach makes it possible to adapt the regulatory burden of the GDPR to the actual risk of the processing, which includes the amount of data to be processed (EDPB 2016). If thus the processing of personal data is not at the center of a company's business model, its effort required to comply with the GDPR can be relatively low. This can be seen differently if the processing entails a high risk for the data subjects despite its small scope (e.g., a company processing sensitive data such as information on health or financial circumstances) or in a way that has a negative effect on data subjects. In such a case, however, the compliance effort is again proportionate due to the increased risk (Schröder 2019).

Second, the GDPR enables controllers and processors to proactively create legal certainty themselves. This is possible by specifying the undetermined provisions of the GDPR in two ways: either in relation to the processing of their specific products or services by means of a certificate, or together with other companies of a certain processing sector by means of a code of conduct (see Art. 40–43 GDPR). In each case, compliance with a certificate or code of conduct is considered to be an important factor in the verification of GDPR conformity (see, for example, Art. 24 (3), Art. 25 (3) and Art. 32 (3) as well as Art. 83 (3) (j) GDPR). In addition, compliance with a certificate or

code of conduct signals compliance with GDPR as a quality feature of their product, service or business to the consumer and/or business customer. Certificates and codes of conduct thus enable both the controller and the processor to reduce their legal uncertainty and to signal their GDPR conformity on the market. Both mechanisms, i.e. higher legal certainty and GDPR compliance as a quality feature, can be used as a competitive advantage for companies (von Grafenstein 2020). Naturally the auditing, which enterprises must accomplish in the context of a certification or a code of conduct, must not be disproportionate in itself. Therefore the GDPR makes explicitly clear that these auditing processes must take the needs of small and medium-sized companies into account (Art. 40 para. 1 a. E. and Art. 42 para. 1 sentence 2 GDPR). Also in this regard, the risk-based approach can play an important role, for example with regard to the depth of such an auditing (von Grafenstein 2020; Kamara 2017). Also, chambers of commerce and business associations play an outstanding role here. The reason for this is that they are mandated to coordinate and represent the interests of their members. Thus, to support their members setting up certificates and, even more so, codes of conduct to meet the society's expectations of them, as well as to exploit competitive advantage, fits well in their mandate.

2.3 Business Associations as Interfaces Between Controllers, IT Providers and Customers: Coordinating the Implementation of Data Protection by Design

Such a coordinating function, for example of business associations, is particularly necessary if several companies must cooperate to implement the GDPR (See Art. 25 GDPR). An important example in this regard are the requirements of data protection by design and security of processing. These provisions require the controller and partially the processor to implement the requirements of the GDPR into the technical and organizational design of their data processing. In most cases, however, the controller uses the technical solutions of third-party providers for its processing activities. These providers are not obliged or to a lesser extent to comply with the GDPR. This leads to the complex situation in which a data controller is primarily legally responsible, but can only fulfil its responsibility with the help of its IT provider. A prominent example for this situation is the Berlin-based property company *Deutsche Wohnen* that was recently fined 14.5 million euros by the Berlin data protection authority, particularly because they did not implement a data deletion concept on their servers. However, such a deletion concept was probably only possible for Deutsche Wohnen by using their third-party provider for their servers (Berlin Commissioner for Data Protection and Freedom of Information 2019). The interplay between the two actors does not seem to have worked sufficiently.

Interestingly, IT providers can use this situation as a competitive advantage or business opportunity. The reason for this is that the main responsible controller must examine carefully which IT provider supports the controller's activities best regarding the technical compliance of the GDPR. With legal questions, such as whether a technology corresponds to the state of the art, also here a certificate or code of conduct can act as an important element between the required and actual state (von Grafenstein 2020). With regard to its focus on the interconnection of business and internet technology, Business Informatics can pave the way for research into the development of such technical-organizational solutions and their effects on economic processes.

2.4 Three Strategies from the Point of View of the Company: From Avoidance and Prevention to Business Opportunity

Following this understanding, both controllers and processors have three basic approaches for dealing with the GDPR in day-to-day business. The first strategy can be described with the expression "burying the head in the sand". Deutsche Wohnen probably applied this approach after the Berlin data protection authority had already pointed out the missing deletion concept during an on-site audit in 2017. The second approach follows the classic compliance logic: A data controller or processor only fulfills the GDPR requirements to the extent that it needs proof to defend itself against a "first-time fine" and immediately implements all additional measures if the competent data protection authority demands them. This approach has the advantage of initially low costs, but carries the risk of a competitive disadvantage if a competitor chooses the third strategy. This third strategy makes a virtue out of a necessity: A data controller or processor uses the leeway that the GDPR gives them to proactively find the best solution for their specific data processing. These controllers and processors see GDPR-compliance as a quality feature for their business customers or end users and generate a competitive advantage from it. This approach requires, however, businesses people – either working in academia or in practice – to see the GDPR not from a classical compliance perspective that hinders innovation but as an aspect in their entrepreneurial environment that they can use as a business opportunity.

3 Challenges with GDPR from the Enterprise Perspective – Building a Dedicated (Personal) Data Management Capability

Christine Legner, Clément Labadie, Faculty of Business and Economics (HEC), University of Lausanne

The GDPR represents a mindset shift in data protection regulation, and the controversial debates have not ended since it came into effect in May 2018. While some of the criticism is justified, the GDPR is a necessary and important step towards establishing data privacy in the digital economy. First, the regulation introduces greater accountability for organizations and enforces established data privacy principles that have hardly been respected in the past. Second, the GDPR gives individuals greater choice and control over their data, and thus promotes their data sovereignty. As the strictest and most farsighted approach to data protection, the GDPR has not only had a major impact on Europe, but also on an international scale and has become a "blueprint" for emerging data protection regulations in other countries.

The GDPR has been heavily criticized, and part of the coverage it has received focuses on the difficulties in implementing it, with many considering the induced strain to be excessive, especially for small and medium size enterprises. Even more than one year after the GDPR came into effect, companies are far from being at ease with the regulation. A study conducted mid-2019 among more than 1100 executives across ten countries and eight sectors reported that only 28% of the responding organizations were compliant with the GDPR at that time, with 30% close to be compliant (Capgemini Research Institute 2019). The study also emphasizes that non-compliance is a worldwide, cross-sector issue, with increasing risks in terms of both direct fine costs and reputational damage. In dealing with the GDPR, enterprises mostly followed a pragmatic approach, addressing visible and pressing compliance issues (e.g. adapting web forms, newsletters and contracts), to achieve a basic level of compliance. However, with this approach, it is almost impossible to address the more sophisticated legal demands, specifically the information processing rights and accountability requirements, or to proactively react to violations. Fortunately, there are also some exceptions; i.e., organizations that are committed to their data responsibility and the ethical treatment of data beyond regulatory requirements, such as Mastercard[1] or Zurich Insurances,[2] that are using data protection as a competitive differentiator.

[1] https://newsroom.mastercard.com/press-releases/mastercard-establishes-principles-for-data-responsibility/.

[2] https://www.zurich.com/en/about-us/corporate-governance/code-of-conduct.

The difficulties with the GDPR can be explained by the changing nature of data protection regulations. In contrast to previous regulations that could be addressed by amending contracts and general conditions, the GDPR requires companies to fundamentally rethink the way they store and process personal data on an enterprise-wide level. Hence, the GDPR is essentially about processing sensitive personal data in the enterprise – and more precisely data about customers, employees and vendors. Achieving enterprise-wide data transparency is challenging for organizations with distributed operations, that, as large as they may be, remain a single point of contact for individuals. Managers often do not have a complete picture of the data stored on heterogeneous systems and do not know how they are used in business processes either. How to correctly handle data access requests if it is not possible to locate all data records? How to explain to individuals how an organization will process their data if nobody actually knows? These questions illustrate the typical difficulties in dealing with the GDPR.

Research in the Competence Center Corporate Data Quality (CC CDQ) reveals that the GDPR requires companies to build a dedicated data management capability (Labadie and Legner 2019). Based on the interpretation of legal texts and practical insights from focus groups and GDPR projects, we identified the required sets of organizational and system capabilities to comply with the regulation. The system capabilities require to redesign data-processing systems and are often emphasized in the GDPR debate. They comprise the abilities (1) to clearly identify, classify and locate personal data in system landscapes (*Manage protected data scope*); (2) to collect consent and ensure consent-based processing of information (*Manage consent*); and (3) to process data according to EU-GDPR's data rights and principles (*Enable data information rights*). Besides these system-related capabilities, the organizational capabilities establish the required processes and responsibilities. They include the abilities (1) to coordinate and execute data protection activities (*Orchestrate data protection activities*); (2) to record and evaluate sensitive processing activities, as well as to document system landscapes (*Demonstrate compliant data processing)*; and (3) to disclose information to individuals and authorities (*Disclose information*). In fact, these capabilities are meant to establish sustained and efficient practices. Implementing these capabilities leads to an enhanced knowledge of personal data in organizations, as well as the way it is used through its processes and systems. We argue in this way it can also support compliance with other regulations, as well as other data-related initiatives.

For the BISE community, the emerging data protection regulations offer interesting research opportunities. From an enterprise perspective, key questions relate to both

organizational and system capabilities and their design for sustainable implementation of regulatory compliance. On the other hand, it would be interesting to conceptualize different levels of compliance for different contexts. Researchers could investigate whether and how data responsibility and ethical treatment of data translate into competitive advantages and operational excellence.

4 Ten Critical Aspects of the European General Data Protection Regulation from the Point of View of Information Systems

Peter Mertens, School of Business, Economics and Society and Faculty of Engineering, University of Erlangen-Nuremberg

1. One critical aspect of the GDPR revolves around the high penalties a violation of this regulation may entail. According to article 83, companies violating the GDPR have to pay a fine of up to 4% of their annual sales. Considering that average profit margins in many economic sectors and industries are about 5%, with relative R&D investments being in a similar range, it becomes obvious that the maximal forfeit of 4% might jeopardize the existence of a firm. This is also why the penalty should be calculated not based on sales but on return on investment (ROI). In Germany, as of yet, the highest penalty amount (14.5 million €) has been imposed on *Deutsche Wohnen*, a German property firm. It had failed to delete files that were no longer needed. The fines associated with the GDPR have thus lead to a strong risk aversion among companies.
2. This risk aversion is further reinforced by legal uncertainty surrounding the GDPR. One reason for this uncertainty relates to the use of vague legal language and terms, such as "legitimate interest,""under consideration of the special circumstances and general requirements,"and "meaningful survey."Another reason, especially for companies operating abroad, relates to so-called "escape clauses" that allow for the integration of country-specific laws and regulations in order to protect national privileges (e.g., freedom of the press). In this context, the EU Commission has criticized that some German regulations appear to be overly tight, while others seem to be overly loose, such as those regulating the appointment of data protection officers in small or medium-sized enterprises (SMEs) (Neuerer 2019). Further, in many functional areas (e.g., human resources) and industries (e.g., healthcare), the GDPR conflicts with the growing number of function- and/or industry-specific rules requiring companies to keep very detailed data records. Also, tax specialists are puzzled by the stark contrast between the far-reaching obligations around data safekeeping, on the one hand, and the „right to be forgotten"stipulated in article 17 of the GDPR, on the other hand. For example, in Germany alone, there are 17 data protection authorities that sometimes contradict each other. Moreover, the enactment of new rules entails reciprocal effects or even additional conflicts. As a consequence, the European Court of Justice limited the "right to be forgotten" to the EU, which implies that Internet firms such as Google are not required to delete 'questionable' links entirely (Wieduwilt 2019). On the other hand, the same court ruled that a user's explicit consent is needed, thereby making it harder for companies to use common web-tracking practices (Ritzer 2019).
3. The complexity of the GDPR also has major implications for the theory and practice of law in general (Kremer 2019; Hey 2019). For example, a survey conducted by BITKOM ("Germany's digital association") revealed that, one year after the GDPR came into effect, only about 25% of surveyed companies had been able to implement the GDPR rules. Additionally, in a related study, 95% of the interviewees indicated that a full implementation of the GDPR would be impossible (BITKOM e.V. 2019).
4. The goal to avoid unpredictable risks has provoked reactions that not always seem to be rational. For example, the explanatory statement of the GDPR suggests that reverting back from electronic files to paper files would not matter, since the regulation is neutral toward the 'technology' used. (More examples can be found in Mertens 2019 and Crocoll 2019.)
5. The GDPR implies a growing burden of fixed costs, mainly resulting from overhead expenses. While large-scale companies can spread these costs across a broad range of related business activities, SMEs often cannot. Thus, the GDPR is another factor promoting market concentration tendencies, which is not desirable in a free-market economy. Moreover, new problems surface in manufacturing units; for instance, errors detected through the collection of data during production may be traced back to flawed customer orders, inaccuracies in production planning and scheduling systems, deficiencies in raw materials and parts purchased from suppliers, logistical problems within the supply chain, as well as mistakes of machine operators. In all these cases, sensitive data may be reviewed by data protection

officers, which in turn would lead to the revelation of company secrets (Mertens 2013; Software AG 2017; Rehaag 2019; Wuhrmann 2019).

6. The legal uncertainty surrounding the GDPR implies that firms active on the Internet will ask users/customers for increasingly detailed and therefore very comprehensive expressions of consent, written in sophisticated legal jargon. Against this backdrop, it would be naïve to assume that users will read this language thoroughly; quite the contrary, most users are likely to merely "click it away"without paying closer attention, also referred to as "tiredness to agree"in recent literature. This is consistent with the general observation that many citizens perceive the GDPR bureaucracy as rather annoying than helpful (Triumph-Adler 2019).
7. In some industries, the GDPR may actually turn into an "innovation barrier". One symptom of such a development can be seen in political efforts in the area of public health to follow through with exceptions for the collection of 'big' patient data in order to not impede R&D efforts concerning computer-assisted diagnosis through artificial neural networks ("balance between protection of data and health"). Here, the German Secretary of Health argues that data protection is "something for healthy people" (Waschinski 2019; Knodt 2019) and has thus initiated the "digital health law".
8. The "backstop" strategies along with the additional costs and potential innovation barriers associated with the GDPR will arguably cause a loss in growth and productivity at the level of the national economy. One indicator for this is the declining number of new start-ups in Germany (− 15% from 2016 to 2018) (Theile and Creutzburg 2019). An interview study with young people found that concerns about data protection bureaucracy represent one key reason for this downward trend (Koch 2019).
9. The manifold drawbacks of the GDPR seem to motivate German politicians to suggest exceptions, for example, related to work safety, finance/taxation, health (see also point 7 above), education (e.g., fine-grained databases to analyze reasons of early school leaving), housing and protection of tenants, homeland security, or defense. For Germany and Austria, one potential solution to this problem may be found in the use of escape clauses (see point 2 above) in order to "take the fright from the GDPR". Or, more generally, to protect citizens and companies alike from 'shady' law firms. In this regard, it is noteworthy that very different organizations – such as the Social Democratic Party (SPD), the Christian Democratic/Social Unions (CDU/CSU), the Association of Self-Employed Entrepreneurs, the Union of Liberal Middle Class, and other powerful interest groups – are aiming at making amendments to the GDPR (Heide and Neuerer 2018). The uncertain outcomes of these efforts, however, further contribute to the overall legal uncertainty.
10. Finally, at a more abstract level, the GDPR mirrors a general problem with the EU: Given the gigantic bureaucracy in Brussels (with around 50,000 people currently being employed across all EU institutions, agencies, and bodies), there are many politicians and employees who – because of their education, socialization, and professional experience – seem to have difficulties in understanding and relating to the day-to-day problems of German entrepreneurs in general, and those of SMEs in particular. This phenomenon, for example, may be explained by Parkinson's law, which has been applied to the growth of bureaucracy in all kinds of organizations.

In conclusion, numerous present challenges resulting from the GDPR can be attributed to the problem that too many guidelines, decrees, and court decisions are intertwined and, in the worst case, contradict one another. In addition, GDPR rules require careful consideration within a short time span, straining the capacities of specialists in corporate management, legislative bodies, public administration, and the system of justice. Recent examples include the EU regulation concerning the use of electronic evidence, the decision of the European Court of Justice concerning the detailed documentation of working hours, the complex regime of country-by-country reporting, the EU guideline PSD2 concerning online payments, the A1 certificate to document the social security status of cross-border commuters, as well as the EU money-laundering guideline. To address existing GDPR challenges, one not trivial but feasible approach might be that the European Commission decided on clear priorities based on urgency. Similar to a state-of-the-art production planning and supply chain system in manufacturing, this approach would help prevent overburdening the above-mentioned national organizations, especially in critical situations, and also help ensure that the overall 'quality' of politics, law, public administration, and corporate management does not suffer.

4.1 What Can BISE Do?

A first step could be to develop a cost–benefit analysis or a forecast of the implications for modules of regulations where several alternatives exist. For example, Germany could have one data protection institution at the federal level versus one data protection office in each state. This task is not trivial, but seems feasible. Maybe knowledge

from the research field „centralization or decentralization of the IT function" could be used.

In a second step, one could aim at transferring knowledge from computer-assisted production planning to something that could be called "computer-assisted legislation planning"or "computer-assisted administration planning". The process could be to develop – together with accountants as well as specialists for production planning in the manufacturing industry and specialists for data processing in public administration – a prototype to adjust the load of new bureaucratic regulations to enterprises of different sectors. This algorithm should be based on empirical estimations of the person-hours in firms of various industries and size. Then the so-called capacity profile can be calculated by adding the capacity needs of different regulations over the time axis. Depending on the results in terms of "summits" and "valleys", the European Commission would plan its own activities, e.g. sessions in the EU-Parliament, and postpone or bring forward the publication and effective date of laws and regulations, whereby the restrictions of the Commission and of the firms should be considered.

5 Information Systems and the General Data Protection Regulation – A Consumer Protection Perspective

Ayten Öksüz – Consumer Association of North Rhine-Westphalia (Verbraucherzentrale Nordrhein-Westfalen)

From the perspective of consumer protection, the General Data Protection Regulation (GDPR; Directive (EU) 2016/679) is a step in the right direction which updates our data legislation. This is why the consumer association of North Rhine-Westphalia welcomes the GDPR. The regulation entails several new principles that aim to empower individuals in gaining more control over their data in a world of growing technological complexities.

5.1 Why is This So Important?

Technologization and digitization are increasingly affecting all areas of life. We shop online, network on social media, use wearables and fitness trackers to keep an eye on our activities and health, and turn the lights on or off with the help of smart speakers. All these new technologies and services can be seen as significant advances which are creating opportunities for people such as simplification of daily life and more convenience.

A side-effect is the great amount of data produced through the use of these numerous smart devices and services. With the help of big data analytics, large volume of data can be examined to bring to light information such as unknown correlations or hidden patterns. On the one hand, this information can be used in a positive way. The application of big data in healthcare, for example, can save life as analyzing specific health data of a population has the potential to prevent epidemics or to cure diseases. On the downside, in many cases, this data is collected and examined by companies, which do not always act transparently. Parts of the data may seem harmless enough on their own. However, most of the consumer data allows companies to draw conclusions about, e.g., personal preferences, lifestyle habits, religious confessions or diseases, which can also have negative consequences for consumers such as unwanted personalized ads, profiling or discrimination (e.g., in terms of insurance). This is why big data also brings along great privacy concerns. Merging and linking user data that was collected over a long period of time and across distinct devices, products or services even intensifies these privacy concerns. As digitization is progressing steadily, data is being collected at an incredible rate, and thus consumers are unable to keep track of which and by whom personal data relating to them is stored and analyzed. A recently published report of Amnesty International even concludes that the business model of Google and Facebook threatens human rights (Amnesty International 2019). In this context, the non-governmental organization warns against – what they call – the "omnipresent surveillance of billions of people".

Therefore, it is necessary to increase the attention everyone pays to data and to reduce bad practice and the bad players by regulating how data is being used in a reasonable, legal and ethical way. This applies to the person who decides on the business model behind an offered service or product as well as to the person who develops the tools, technologies, and algorithms capturing and analyzing data about their users. The GDPR opens up new possibilities to deal with these emerging challenges by making it easier to demand greater transparency and accountability from those who collect and use data. It also provides consumers with more control over their data. For example, requirements for the comprehensibility of privacy policies have increased and information about how and by whom data is collected and used has to be properly disclosed to consumers. Companies that violate the principles of GDPR face higher monetary penalties so that also big players in the market, which do not act in accordance to data protection law yet, are now forced to change their behavior. According to the "privacy by default" obligation, which is one of the key requirements of the GDPR, data controllers must implement appropriate technical and organizational measures ensuring that only such personal data is collected that is necessary for the specific purpose mentioned. Thus, the minimum amount of personal data

required should be collected. Overall, GDRP strengthens consumers' fundamental rights in the digital age. So much for the theory.

Unfortunately, practice still looks a bit different. In 2018, as part of the project "Market Watch Digital World", the Consumer Association of North Rhine-Westphalia (Verbraucherzentrale NRW) investigated how certain social media providers deal with selected rules of the GDPR (Moll et al. 2018). The results show a poor implementation of the GDPR by the examined social media providers. Privacy policies contain vague and unclear wording so that consumers still can hardly understand, how and by whom their data is being processed and used. Regarding "privacy by default", there is also still some catching up to do. Default settings users are confronted with during the account registration often are not privacy-friendly. For example, with most of the examined social media services, user-generated content is publicly visible by default rather than only visible for contacts selected by the respective user. Furthermore, the majority of the social media providers monitors their users' browsing activities by default and analyzes the collected data to serve personalized advertising.

In addition, the Market Watch Digital World team tested how selected social media providers respond to "request of information" and "request of getting a copy of personal data" (Scheibel et al. 2019). As stated in the GDPR, users (in the GDPR called "data subject") have the right to obtain from, e.g., a service provider confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, they have the right to access the respective personal data. As part of the "right to data portability", which is another key new principle that has been included in the GDPR, users have the right to receive a copy of their personal data in a structured, commonly used and machine-readable format. However, results of the test show that most of the social media providers answered inadequately. They solely referred to their general privacy policies or to their support site instead of giving the specifically requested information as provided by the GDPR. With regard to the "request of getting a copy of personal data", some of the social media providers sent a link for downloading personal data stored about the respective user. However, in most of the cases, downloaded data was only available in unstructured form and various file formats that, partially, could not be opened with standard software. Thus, consumers are not able to use the downloaded data packets in order to make informed decisions regarding the transmission of their data to, for example, another social media provider.

Other studies, such as the one conducted by researchers of the University of Göttingen commissioned by the Federal Ministry of Justice and Consumer Protection (Wiebe and Helmschrot 2019), also conclude that there is still a lot to do when it comes to the practical implementation of GDPR. One important step in this connection would be to equip responsible parties such as data protection authorities with adequate resources to facilitate a stronger enforcement of GDPR. Only if requirements are consistently implemented by service providers or data controllers will consumers be able to exercise their rights in practice so that GDPR can achieve the desired effects.

6 The GDPR from a Perspective of Consumer Informatics

Gunnar Stevens, Information Systems esp. IT-Security and Privacy, University of Siegen

From the point of view of consumer informatics, the General Data Protection Regulation (GDPR) represents an important step towards the reorganization of data protection for a digital society. A statement from the point of view of consumer informatics can be related to two levels: Firstly, it can address the level of the concrete organization and conversion. There is certainly much that can be criticized here, e.g. whether the threats of punishment are appropriate, whether companies have been granted sufficient transitional periods, etc. In contrast, this contribution focuses on the second, the conceptual level and the spirit behind the GDPR.

In times of data capitalism and the increase of AI procedures in application systems, it is important to remember that from this point of view and for a modern, liberal society the principle of informational self-determination is a great asset, which is by no means natural, but must always be defended anew.

For individual mental hygiene, but also for social participation and political decision-making, citizens need retreats in which they are unobserved and can express themselves freely. This need is protected by the state through a number of defensive rights, such as the inviolability of homes or the secrecy of telecommunications. To the extent that life practices become digital, corresponding retreats are needed in the digitalized world. To secure such spaces and promote informational self-determination, three essential aspects are mentioned here as examples.

6.1 Access and Processing Control

Privacy is traditionally thought of in terms of space – it is therefore usually created by a physical access restriction or access control. The fact that consumer life increasingly takes place in the digital world (e.g., in social media and messengers) and at the same time existing places considered private are becoming "smart" (e.g., the home or the

private car) poses new challenges for effective and usable access restrictions and controls.

It is therefore to be welcomed that GDPR prescribes a minimization of processing and storage of personal data in the interests of data economy and that data must be secured in accordance with the state of the art. Both aspects strengthen access restrictions and minimize the risk of unauthorized access. The general principle that data must be collected and processed for a specific purpose is also to be welcomed. The informed consent of the data subject, which can be revoked at any time, also strengthens control over the data and constitutes an essential cornerstone of informational self-determination.

6.2 Prohibition of Coupling and the Right to Unobserved Use

Informational self-determination presupposes the voluntariness of consent. Voluntariness, by nature, requires a prohibition of coupling, meaning that the provision of a service must not depend on consent for the processing of data, or said processing must be limited to the execution of the contract or the provision of the service itself. This should be the guiding principle when designing new services and data-supported business models.

This prohibition of coupling is becoming increasingly important as more and more areas of life are digitized and social participation increasingly depends on the use of digital services. This starts with legally binding services such as networked electricity meters, the eCall service in the car or digitally connected health insurance cards, and continues with the use of more and more important but oligopolistic services such as Google Search, Android/iOS, Facebook, WhatsApp and Amazon for social participation. Due to their importance for social coexistence, it is not possible to speak of voluntary use in the sense of informational self-determination. Accordingly, it should apply in principle that services that are legally obligatory, that are part of services of general interest, or that are central to social participation, must be usable in a way that protects privacy. The question is not whether someone subjectively believes that he or she is actually able to use the service voluntarily, but whether non-use would entail considerable losses for the lives of those affected. In the case of such services, the processing and storage of personal data must be limited to their provision and the execution of contracts. Purposes beyond this must be agreed to by the user and must not be linked to the provision of the service.

6.3 Information Rights and Information Asymmetries

The story of Mr. K. in Kafka's Process can be viewed as a parable about the negative consequences of automated decision-making processes in times of AI and Big Data: *He is arrested without being aware of any guilt. Above all, he is not told why he was charged and how he could justify himself.*

In research on computer supported collaborative work (CSCW), the meaning of the "I understand how the other understands me" principle has long been known. It is an important prerequisite for social action to coordinate, to negotiate roles and, as in K.'s case, to justify or claim justifications. Here lies the essential strength and progress of the GDPR: not to reduce data protection to the term "privacy", which is common in the English-speaking world, but to develop it further in the direction of digital consumer protection. The aim is transparency as to how government agencies and companies use personal data and how data-supported decisions are made. In particular, the regulation regarding the right to access data and the right of consumers not to be subject to automated processing – including profiling – should be mentioned here.

In future, however, both rights should be developed more consistently towards the above "I understand how the other understands me" principle in order to reduce information asymmetry. Knowing what data is collected about you is only the first step. In order to adequately assess risks, it is necessary to make (semi-)automated decision-making processes and their procedures transparent for those affected, as well as to be able to control the associated systems through an independent body.

6.4 Standardized, Machine-Readable Consumer Data

The provision of data in machine-readable, standardized formats is important from the point of view of consumers in two respects. On the one hand, this reduces lock-in effects and opens up new possibilities for consumers to provide this data to other value-added service providers (e.g., fitness trackers and shopping histories can be used by general practitioners and nutritionists to provide more targeted information on healthy lifestyles). On the other hand, consumers can make this data available to so-called legaltech service providers so that these can easily enforce their rights, cancel contracts or change suppliers on behalf of consumers.

6.5 Implementation and Research Needs

A number of practical problems have been identified during implementation, such as how to ensure that data subjects are well informed, how to avoid a flood of information when using dozens of services, and how to implement information management in practice by keeping (revoked) consents, purposes and data consistent and up to date. The situation is made more difficult by the fact that

both the data subjects and the companies do not know exactly what information is contained in the data and for what purpose it can be used. Another example for this is the right of information, in which companies and authorities use a proliferation of requirements for authentication, processes, contact points and data formats that consumers have to deal with. These range from digital formats of spreadsheet programs to PDFs and paper printouts. The list could be continued.

Accordingly, design-oriented business and consumer informatics should take up the ball and develop standardized formats for consumer data as well as reference models for the usable information process. On the other hand, it should conduct research with industry and consumer protection organizations on innovative solutions for access and processing control that take the interests of the various parties, including consumers, into account in an appropriate manner in the interests of multilateral security.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Albrecht JP (2016) How the GDPR will change the world. Eur Data Prot Law Rev 2:287–289

Alizadeh F, Jakobi T, Boldt J, Stevens G (2019) GDPR-reality check on the right to access data: claiming and investigating personally identifiable data from companies. In: Proceedings of Mensch und Computer 2019. ACM, New York, pp 811–814

Alvarez SA, Barney JB (2007) Discovery and creation: alternative theories of entrepreneurial action. Strateg Entrep J 1:11–26

Amnesty International (2019) Surveillance giants: how the business model of Google and Facebook threatens human rights. https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF. Accessed 9 Feb 2020

Berg-Larsen E (2015) The issue of privacy in the European Union – controversies of the General Data Protection Regulation. Master's Thesis, University of Oslo

Berlin Commissioner for Data Protection and Freedom of Information (2019) Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf. Accessed 3 Dec 2019

Capgemini Research Institute (2019) Championing data protection and privacy. https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/09/Report_GDPR_Championing_DataProtection_and_Privacy.pdf. Accessed 9 Feb 2020

Crocoll S (2019) Der Schatz aus der Maschinenhalle. In: Wirtschaftswoche No. 13, 22 Mar 2019, pp 29–31

Cvik ED, Pelikánová RM, Malỳ M (2018) Selected issues from the dark side of the General Data Protection Regulation. Rev Econ Perspekt 18:387–407

De Hert P, Papakonstantinou V (2016) The new General Data Protection Regulation: still a sound system for the protection of individuals? Comput Law Secur Rev 32:179–194

De Hert P, Papakonstantinou V, Malgieri G et al (2018) The right to data portability in the GDPR: towards user-centric interoperability of digital services. Comput Law Secur Rev 34:193–203. https://doi.org/10.1016/j.clsr.2017.10.003

Degeling M, Utz C, Lentzsch C et al (2018) We value your privacy… Now take some cookies: measuring the GDPR's impact on web privacy. arXiv:180805096

Diker Vanberg A, Ünver MB (2017) The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo? Eur J Law Technol 8(1):1–22

EDPB (2016) Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation. Data Protection Working Party 2016/679, 5:10. Accessed 9 Feb 2020

Eifert M, Hoffmann-Riem W, Schmidt-Aßmann E, Voßkuhle A (2012) Regulierungsstrategien. In: Grundlagen des Verwaltungsrechts. Bd. I „Methoden – Maßstäbe – Aufgaben – Organisation", 2nd edn. Beck, München

Ermakova T, Fabian B, Bender B, Klimek K (2018) Web tracking – a literature review on the state of research. In: Proceedings of the 51st Hawaii international conference on system sciences. https://doi.org/10.24251/hicss.2018.596

European Parliament and Council (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Off J Eur Union Law 119/2016, vol 59

Fox G, Tonge C, Lynn T, Mooney J (2018) Communicating compliance: developing a GDPR privacy label. In: 24th Americas conference on information systems, New Orleans

Gartner WB (1985) A conceptual framework for describing the phenomenon of new venture creation. Acad Manag Rev 10:696–706

Gellert R (2018) Understanding the notion of risk in the General Data Protection Regulation. Comput Law Secur Rev 34:279–288

Hartog C, Van Stel A, Storey DJ (2011) Institutions and entrepreneurship: the role of the rule of law; levie, autio, regulatory burden, rule of law, and entry of strategic entrepreneurs: an international panel study. J Manag Stud 48(6):1392–1419

Heide D, Neuerer D (2018) Parteiübergreifende Kritik am neuen Datenschutz. Handelsblatt 13 June 2018, p 9

Hey J (ed) (2019) Digitalisierung im Steuerrecht. Schmidt, Köln

Hintze M, El Emam K (2018) Comparing the benefits of pseudonymisation and anonymisation under the GDPR. J Data Prot Priv 2(2):145–158

Hoffmann-Riem W (2006) Innovationsoffenheit und Innovationsverantwortung durch Recht: Aufgaben rechtswissenschaftlicher Innovationsforschung. Archiv des öffentlichen Rechts 131:255–277

Huth D (2017) A pattern catalog for GDPR compliant data protection. In: Ralyté J, Roelens B, Demeyer S (eds): Proceedings of the doctoral consortium and industry track papers presented at the 10th IFIP WG 8.1 working conference on the practice of enterprise modelling (PoEM 2017), Leeuven, pp 34–40

Jaeckel L (2010) Gefahrenabwehrrecht und Risikodogmatik – Moderne Technologien im Spiegel des Verwaltungsrechts. Mohr Siebeck, Tübingen

Jakobi T, Patil S, Randall D et al (2019a) It's about what they could do with the data: a user perspective on privacy in smart metering. ACM Trans Comput Hum Interact 9:43. https://doi.org/10.1145/3281444

Jakobi T, Stevens G, Seufert A-M, Becker M (2019b) Webtracking under the new data protection law: design potentials at the intersection of jurisprudence and HCI. In: Proceedings of Mensch und Computer 2019. ACM, New York, pp 309–319

Kamara I (2017) Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. Eur J Law Technol 8(1):4

Karyda M, Mitrou L (2016) Data breach notification: issues and challenges for security management. In: Proceedings mediterranean conference on information systems, p 60. https://aisel.aisnet.org/mcis2016/60

Knodt M (2019) Hürden für Dr. Algorithmus. Handelsblatt 15 Oct 2019, p 13

Koch M (2019) Wenig Gründermut. Handelsblatt 2 Sept 2019, p 8

Kremer S (2019) Ein Jahr DSGVO: Aktuelle Entwicklungen und Herausforderungen des neuen Datenschutzrechts in der Praxis. In: Der Betrieb No. 25, 24 June 2019, pp 1429–1435

Labadie C, Legner C (2019) Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR, In: Internationale Tagung Wirtschaftsinformatik 2019. https://wi2019.de/wp-content/uploads/Tagungsband_WI2019_reduziert.pdf. Accessed 10 Feb 2020

Lachaud E (2018) The General Data Protection Regulation and the rise of certification as a regulatory instrument. Comput Law Secur Rev 34:244–256

Lambrinoudakis C (2018) The General Data Protection Regulation (GDPR) era: ten steps for compliance of data processors and data controllers. In: International conference on trust and privacy in digital business. Springer, Heidelberg, pp 3–8

Legner C, Eymann T, Hess T et al (2017) Digitalization: opportunity and challenge for the business and information systems engineering community. Bus Inf Syst Eng 59:301–308

Levie J, Autio E (2011) Regulatory burden, rule of law, and entry of strategic entrepreneurs: an international panel study. J Manag Stud 48:1392–1419

Lopes IM, Guarda T, Oliveira P (2019) How ISO 27001 can help achieve GDPR compliance. In: 14th Iberian conference on information systems and technologies (CISTI). Coimbra, pp 1–6. https://doi.org/10.23919/cisti.2019.8760937

Mayer-Schonberger V (2010) The law as stimulus: the role of law in fostering innovative entrepreneurship. I/S J Law Policy Inf Soc 6:153

Mertens P (2013) Integrierte Informationsverarbeitung. 1. Operative Systeme in der Industrie, Chapter 3.5.2.9, 18th edn. Springer, Heidelberg

Mertens P (2019) Die Datenschutz-Grundverordnung – eine kritische Sicht. Wirtschaftsinformatik und Management 11(1):6–17

Mhaidli AH, Zou Y, Schaub F (2019) "We can't live without them!" App developers' adoption of ad networks and their considerations of consumer risks. In: Proceedings of the 15th USENIX conference on usable privacy and security. USENIX Association, pp 225–244

Mitrou L (2017) The General Data Protection Regulation: a law for the digital age? In: Synodinou TE et al (eds) EU Internet Law. Springer, Heidelberg, pp 19–57

Moll R, Horn M, Scheibel L, Rusch-Rodosthenous M (2018) Informationspflichten und datenschutzfreundliche Voreinstellungen. Soziale Medien und die EU-Datenschutzgrundverordnung. Verbraucherzentrale NRW e. V. (Hrsg.). https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_i.pdf. Accessed 12 Feb 2020

Neuerer D (2019) Weniger ist mehr. Handelsblatt 20 Sept 2019, p 16

Politou E, Alepis E, Patsakis C (2018) Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. J Cybersecur 4:tyy001

Rehaag C (2019) Neuer Geheimnisschutz. Frankfurter Allgemeine Zeitung 19 June 2019, p 18

Riedl R, Benlian A, Hess T et al (2017) On the relationship between information management and digitalization. Bus Inf Syst Eng 59:475–482. https://doi.org/10.1007/s12599-017-0498-9

Ritzer C (2019) Keine Harmonie bei Cookies. Frankfurter Allgemeine Zeitung 9 Oct 2019, p 16

Scheibel L, Horn M, Öksüz A (2019) Recht auf Auskunft und Datenübertragbarkeit. Soziale Medien und die EU-Datenschutzgrundverordnung. Verbraucherzentrale NRW e. V (ed). https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_ii.pdf. Accessed 12 Feb 2020

Schelter S, Kunegis J (2018) On the ubiquity of web tracking: insights from a billion-page web crawl. J Web Sci 4:53–66

Schröder M (2019) Der risikobasierte Ansatz in der DS-GVO – Risiko oder Chance für den Datenschutz. Zeitschrift für Datenschutz 9:503–506

Schumpeter J (2003) Capitalism, socialism and democracy. 5th edn. Routledge, New York

Software AG (2017) Ensuring compliance with the General Data Protection Regulation (GDPR). Software AG, Darmstadt

Tankard C (2016) What the GDPR means for businesses. Netw Secur 2016:5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

Theile G, Creutzburg D (2019) Die Deutschen scheuen das Risiko. Frankfurter Allgemeine Zeitung 16 August 2019, p 15

Triumph-Adler (2019) Datenschutz: Kein Grund zur Panik. https://triumph-adler.de/ta-de-de/talking-future/undesgehtdoch-leben-mit-DSGVO. Accessed 26 Nov 2019

Urbach N, Ahlemann F, Böhmann T et al (2019) The impact of digitalization on the IT department. Bus Inf Syst Eng 61:123–131

Utz C, Degeling M, Fahl S et al (2019) (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings of the ACM SIGSAC conference on computer and communications security. ACM, New York, pp 973–990

Voigt P, Von dem Bussche A (2017) The EU General Data Protection Regulation (GDPR). A practical guide. Springer, Cham

von Grafenstein M (2020) 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. In: González-Fuster G, van Brakel R, De Hert P (eds) Research handbook on privacy and data protection law. Values, norms and global politics. Elgar, Cheltenham

Waschinski G (2019) Spahn plant eigenes Datenschutzgesetz. Handelsblatt 5 July 2019, p 12

Wiebe A, Helmschrot C (2019) Untersuchung der Umsetzung der Datenschutz-Grundverordnung (DSGVO) durch Online-Dienste. https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/112919_DSGVO_Studie.pdf. Accessed 12 Feb 2020

Wieduwilt H (2019) Gerichtshof begrenzt das Vergessen im Internet auf die EU. Frankfurter Allgemeine Zeitung 25 Sep 2019, p 17

Wuhrmann D (2019) Plattform für den Autobau. Frankfurter Allgemeine Zeitung 19 June 2019, p 18

Zarsky TZ (2016) Incompatible: the GDPR in the age of big data. Seton Hall Law Rev 47:995–1020