Research Paper-Special Issue on "Regulation in the Age of Digitalization"

JIT

Journal of Information Technology
2023, Vol. 0(0) 1–29

DOI: 10.1177/02683962221141456
Journals.sagepub.com/jinf

Building data management capabilities to address data protection regulations: Learnings from EU-GDPR

Clément Labadie and Christine Legner

Abstract

The European Union's General Data Protection Regulation (EU-GDPR) has initiated a paradigm shift in data protection toward greater choice and sovereignty for individuals and more accountability for organizations. Its strict rules have inspired data protection regulations in other parts of the world. However, many organizations are facing difficulty complying with the EU-GDPR: these new types of data protection regulations cannot be addressed by an adaptation of contractual frameworks, but require a fundamental reconceptualization of how companies store and process personal data on an enterprise-wide level. In this paper, we introduce the resource-based view as a theoretical lens to explain the lengthy trajectories towards compliance and argue that these regulations require companies to build dedicated, enterprise-wide data management capabilities. Following a design science research approach, we propose a theoretically and empirically grounded capability model for the EU-GDPR that integrates the interpretation of legal texts, findings from EU-GDPR-related publications, and practical insights from focus groups with experts from 22 companies and four EU-GDPR projects. Our study advances interdisciplinary research at the intersection between IS and law: First, the proposed capability model adds to the regulatory compliance management literature by connecting abstract compliance requirements to three groups of capabilities and the resources required for their implementation, and second, it provides an enterprise-wide perspective that integrates and extends the fragmented body of research on EU-GDPR. Practitioners may use the capability model to assess their current status and set up systematic approaches toward compliance with an increasing number of data protection regulations.

Keywords

EU-GDPR, data protection, regulations, compliance, resource-based view, capabilities

Introduction

In 2020, the European Commission (EC) released a plan for a European data strategy. This plan outlines the transformative importance of data in modern economies and strives to position the European Union (EU) at the forefront of data-related innovation (European Commission, 2020). One of the pillars of this strategy is the building of public trust in data processing activities, with the General Data Protection Regulation (EU-GDPR) enabling individuals to have control over their personal data. EC President Ursula von der Leyen even expressed the hope that the EU-GDPR would set data protection *"standards for the rest of the world"* (von der Leyen, 2020). Since it went into effect in May 2018, the EU-GDPR has initiated a paradigm shift in data protection toward greater choice and sovereignty for individuals and more accountability for organizations (De Hert and Papakonstantinou, 2012). The strict European rules have inspired regulations in other parts of the world, for instance, the California Consumer Privacy Act (CCPA, California State Senate, 2018), India's new Personal Data Protection Bill (Parliament of the Republic of India, 2018, Govindarajan et al., 2019), and Japan's update to the Act on the Protection of Personal Information (Japan Personal Information Protection Commission, 2020, Tanaka and Kitayama, 2020).

Faculty of Business and Economics (HEC), University of Lausanne, Switzerland

Corresponding author:
Christine Legner, Faculty of Business and Economics (HEC), University of Lausanne, Internef 127.3, Lausanne 1015, Switzerland.
Email: christine.legner@unil.ch

For organizations, these regulations come with a mandate to clarify whether, how, and how well they protect personal data, along with increased fines for non-compliance. As they apply at a scale larger than any previous data protection regulations, they require a fundamental reconceptualization of how they store and process personal data on an enterprise-wide level. In the case of EU-GDPR, many organizations are still facing significant compliance challenges and struggle with the conflicting interests between legal obligations, business drivers, and innovation (Jakobi et al., 2020). A study conducted in June 2019 among more than 1000 European and US companies reported that organizations had been overoptimistic about their ability to achieve timely compliance. When surveyed in March and April 2018, 78% of responding organizations expected to comply with the EU-GDPR by the time it came into force, but only 28% of them reported being compliant when evaluated a year later (Capgemini Research Institute, 2019). A study released in April 2020 reveals similar difficulties among multinational enterprises: Only 54% of them had achieved operational compliance, while 37% were still conducting "significant readiness actions," and 9% were still in "project mode" (Dansac Le Clerc and Mannent, 2020). According to this study, a majority of organizations are still implementing mechanisms to manage data protection rights, data storage and retention, and in-depth registries of data processing activities (Dansac Le Clerc and Mannent, 2020).

From a research perspective, the EU-GDPR has been debated in both legal and IS communities (De Hert and Papakonstantinou, 2012, 2016; Jakobi et al., 2020; Mitrou, 2017). Although legal aspects of information privacy had not been among the "topic areas closer to the interests of most IS researchers" (Bélanger and Crossler, 2011), the EU-GDPR has recently attracted more academic interest. Like the idea of regulatory technologies for financial regulations, so-called "RegTech" (Butler and O'Brien, 2019), IS researchers have mostly focused on technical solutions that ease EU-GDPR compliance, such as blockchain (Farshid et al., 2019; Guggenmos et al., 2020; Mejtoft et al., 2019; Rieger et al., 2019) or enterprise architecture (Burmeister et al., 2019, 2020; Huth, Burmeister, et al., 2020). In doing so, the existing body of IS research on EU-GDPR remains fragmented and proposes solutions for isolated aspects of the regulation. It fails to provide an enterprise-wide perspective on the compliance requirements and a broader discussion of the alternative ways to address them.

The difficulties in achieving EU-GDPR compliance highlight the general lack of common ground not only between legal and IS research communities but also between professionals in both disciplines. In most companies, data protection topics have traditionally been addressed by legal and compliance departments, which adapt contracts and general conditions. The new generation of data protection regulations does not allow for such a restricted approach, but requires a fundamental reconceptualization of how companies store and process personal data on an enterprise-wide level (Labadie and Legner, 2020). Since the EU-GDPR does not prescribe concrete implementation options, companies find it challenging to interpret the regulation and develop suitable data management practices that support compliance. Thus, data processing–related issues remain the most challenging topics in the EU-GDPR (De Hert and Malgieri, 2018; Nicolaidou and Georgiades, 2017; Thélisson, 2020).

In this paper, we introduce the resource-based view (RBV) as a theoretical lens that helps explaining the complex and lengthy trajectories towards EU-GDPR compliance. We argue that companies have to mobilize technological, human, and intangible resources and build dedicated, enterprise-wide data management capabilities in order to reach their regulatory compliance objective—or, as conceptualized by Sadiq et al. (2007) their "control objectives." The latter are directly or indirectly related to firm performance, as non-compliance may have significant direct (e.g., fines) and indirect (e.g., reputation loss) financial consequences. Using the RBV also allows extending the regulatory compliance management (RCM) literature (Abdullah et al., 2009; Cleven and Winter, 2009; El Kharbili, 2012), which provides systematic approaches to analyzing regulations, but has not yet embraced the EU-GDPR. Here, capabilities can serve as a way to translate abstract compliance requirements into routines and practices.

More specifically, this paper addresses the following research question: *What data management capabilities need to be built to address the EU-GDPR's requirements?* Following a rigorous design science research process (Peffers et al., 2007), we propose a capability model for the EU-GDPR that synthesizes three groups of capabilities—that is, infrastructure, management, and external linkages—that organizations must build to comply with the regulation. The capability model was iteratively developed based on the interpretation of legal texts, findings from EU-GDPR-related publications, and practical insights from focus groups with experts from 22 companies and four EU-GDPR projects[1]. We find that capabilities can create "common ground" between legal and IS perspectives: they help analyzing compliance requirements and discussing ways to address them before a decision is made on concrete (technical) implementations.

By providing a comprehensive, theoretically and empirically grounded capability model for the EU-GDPR, our study advances interdisciplinary research at the intersection between IS and law with two types of contributions: First, it contributes to the research on regulations, a topic that has seen few contributions in the IS domain in the past but is enjoying a renewed interest in the context of digitalization and Big Data. Specifically, it connects the nascent research on EU-GDPR to the regulatory compliance management

literature (Abdullah et al., 2009; Cleven and Winter, 2009; El Kharbili, 2012). It establishes a link between compliance rules and practice in the spirit of the sense-making dimension of IT-based regulation (de Vaujany et al., 2018). Second, our study complements the fragmented research on the EU-GDPR that treats selected aspects of the regulation or proposes specific implementation solutions by providing an integrated, enterprise-wide perspective. The capability model acts as an overarching framework that outlines the links between compliance requirements, capabilities, and their materialization in the form of resources. It allows researchers to theorize about the capabilities required for EU-GDPR-compliant data management, position and compare their suggestions for EU-GDPR-compliant solutions in the larger context and generalize beyond the EU-GDPR. Practitioners may use the capability model to assess their current status and set up systematic approaches toward compliance with an increasing number of data protection regulations.

The remainder of this paper is structured as follows: We start by introducing the EU-GDPR and providing a synthesis of research on the topic, as well as regulatory compliance in general. After outlining the research methodology and process, we motivate the RBV perspective and present the capability model. We conclude by summarizing our contribution and discussing future research.

Background and related research

Paradigm shift in data protection regulations

In January 2012, the European Commission published a proposal for an overhaul of data protection law, which would become the EU-GDPR[2]. The aim was to remedy the fragmented implementations of the previous Data Protection Directive (95/46/EC) and account for the significant changes introduced by the Internet and digital services (Mitrou, 2017; Nicolaidou and Georgiades, 2017). The EU-GDPR is noteworthy for successfully harmonizing the European data protection legal framework and applies directly in all 27 EU member states, a scale much larger than any previous data protection regulation. Moreover, its relevancy extends beyond Europe: On the one hand, any organization that processes the personal data of an EU citizen must comply with it regardless of the geographical location of their operations. If it fails to do so, significant fines will be imposed (i.e., up to 20 million euros or 4% of an organization's global revenues, whereas previous regulations averaged at around 500,000 euros). On the other hand, the EU-GDPR has been conceived as a worldwide reference for data protection (von der Leyen, 2020), and the strict European rules have inspired data protection regulations in areas of the world that did not have any, such as the California Privacy Act (CCPA) and India's Personal Data Protection Bill (Parliament of the Republic of India, 2018). In the United States, there have been official calls to complement domain-specific provisions, such as the Health Insurance Portability and Accountability Act (HIPAA) for health information, with a full-fledged data protection regulation at the federal level, similar to the EU-GDPR (Rubio, 2019). Other countries, such as Japan (Japan Personal Information Protection Commission, 2020) and Switzerland (Swiss Confederation, 2020), have been compelled to update their existing data protection frameworks to match the EU-GDPR's strengthened requirements (Métille and Raedler, 2017, Tanaka and Kitayama, 2020). These developments are a testimony to the EU-GDPR's global influence and show that it has become the de facto standard for data protection (De Hert and Malgieri, 2018, Thélisson, 2020).

While these new regulations reinforce established data protection concepts (Debet, 2018, Wiese Schartum, 2018), they also introduce a paradigm shift toward greater choice and sovereignty for individuals and more accountability for organizations (De Hert and Papakonstantinou, 2012, 2016; Mitrou, 2017). Most notably, they strengthen existing transparency mandates—in the case of the EU-GDPR, organizations must inform individuals about data processing in clear language and separately from general conditions. They are also required to present more granular consent options (Nicolaidou and Georgiades, 2017). One of the major additions is the concept of accountability, which implies that organizations must be able to demonstrate compliance with the regulation. They must also appoint data protection officers (DPOs) and announce data breaches to both authorities and individuals. Privacy-by-design principles (i.e., implementing privacy from the ground up in systems and offerings) also appear in the regulation, along with new individual rights, such as data portability and a right to oppose automated decision making (Nicolaidou and Georgiades, 2017).

EU-GDPR and data protection in IS literature

Although the EU-GDPR was finalized in 2016 and entered into force in May 2018, it was slow to attract the attention of IS researchers. This mirrors a general reluctance among IS researchers to probe information privacy (Bélanger and Crossler, 2011). In 2018, a query with the keyword "GDPR" on the AIS Electronic Library only returned 27 matches. This number has increased tenfold in the past two years, resulting in 262 matches at the end of 2020. A more detailed review of these studies reveals four categories of contributions, but only the first two categories treat the EU-GDPR as their central topic of interest (see Table 1):

1. *Overall regulation* (19 studies; for details, see Table 1): These studies analyze the regulation as a

Table 1. Overview of EU-GDPR related studies in IS literature.

Study	Type*	Topic area†	Research focus
Scope: overall regulation			
Addis and Kutar (2018)	C	Impact	Impact of EU-GDPR on emerging technologies
Martin and Matt (2018)	E	Impact	Impact of privacy regulations on startup innovation
Pankowska (2018)	C + E	Practices	EU-GDPR mapping to privacy frameworks and awareness
Russell et al. (2018)	C	Impact and practices	Transformation framework for digital privacy
Tona et al. (2018)	C	Tech./Tools	Design of ethical Big Data artifacts
Veiga et al. (2018)	E	Practice	Mapping of data protection regulations and benchmarking of practices
Burmeister et al. (2019)	C	Tech./Tools	Enterprise architecture metamodel for EU-GDPR
Martinez et al. (2019)	C	Impact	Impact of EU-GDPR on smart grid operations
Rösch et al. (2019)	C	Tech./Tools	Translation of legal requirements into technical requirements
Addis and Kutar (2020)	E	Tech./Tools	Data protection challenges arising from AI implementation
Burmeister et al. (2020)	C	Tech./Tools	Enterprise architecture management supporting EU-GDPR implementation
Francis et al. (2020)	C	Practices	Comparison of principles behind privacy frameworks in 14 countries
Grundstrom et al. (2020)	E	Practices	EU-GDPR impact on access to data inside organizations
Houta et al. (2020)	E	Concerns	Analysis of EU-GDPR discourse on social media
Huth, Burmeister (et al. (2020)	E	Practices	Collaboration between legal and enterprise architecture teams during EU-GDPR implementation
Jakobi et al. (2020)	C	Impact	Research contribution regarding conflicting business implications of EU-GDPR implementation
Lindgren (2020)	E	Impact	Impact of EU-GDPR on (multi–)business model innovation
Maunula (2020)	C	Tech./Tools	Technology review for EU-GDPR
Zhang et al. (2020)	E	Concerns	Impact of EU-GDPR on consumer online trust
Scope: data protection rights			
Engels (2016)	C	Impact	Impact of data portability right on competition dynamics
Farshid et al. (2019)	C	Tech./Tools	Blockchain prototype for data deletion
Presthus and Sørum (2019)	E	Concerns	Privacy awareness and knowledge of consumers following EU-GDPR
Rieger et al. (2019); Guggenmos et al. (2020)	E	Tech/Tools	Design principles and development of blockchain solution for asylum procedures in Germany
Wohlfarth (2019)	C	Impact	Strategic aspects of data portability
Scope: consent			
Bergram et al. (2020)	E	Attitudes	Influence of phrasing and digital nudges on user consent and privacy awareness
Kurtz et al. (2020)	E	Practices	Identification of consent-related issues and design goals
Proferes and Walker (2020)	E	Attitudes	Researchers' attitudes toward consent in exploiting public data
Scope: transparency requirements			
Alboaie (2017)	C	Tech./Tools	Privacy label for GDPR
Diamantopoulou and Mouratidis (2018)	C	Tech./Tools	Reference architecture for privacy-level agreements
Fox et al. (2018)	C	Tech./Tools	Guidelines for compliant privacy notices
Mejtoft et al. (2019)	E	Tech./Tools	Blockchain prototype for increased transparency of data processing
Watson and Nations (2019)	E	Tech./Tools	Identification of factors influencing transparency of algorithms and recommendations
Paul et al. (2020)	E	Impact	Impact of EU-GDPR on user privacy perceptions for wearable IoT devices
Scope: accountability requirements			
Karyda and Mitrou (2016)	C	Practices	Information security/incident management
Petkov and Helfert (2017)	E	Practices	Applying data breach notification to past infringements
Kurtz et al. (2018)	E	Practices	Review of third-party data processors
Vemou and Karyda (2018)	C	Practices	Evaluation of privacy impact assessment methods
Kurtz et al. (2019)	E	Practices	Analysis of third-party data processing in service ecosystems

(continued)

Table 1. (continued)

Study	Type*	Topic area†	Research focus
Scope: technical and organizational measures			
Huth and Matthes (2019)	C	Tech./Tools	Privacy engineering approaches for software development
Faber et al. (2020)	C	Tech./Tools	Blockchain-based personal data and identity management system
Huth, Both et al. (2020)	C	Tech./Tools	Tool prototype and approach for integrating privacy aspects in agile development methods

*C = conceptual, E = empirical.
†Based on Bélanger and Crossler (2011).

whole. Most popular contributions relate to the EU-GDPR's impact and mapping of the regulation to existing domain-specific frameworks. This is where we position the study at hand.

2. *Selected aspects of the regulation* (23 studies; for details, see Table 1): These studies treat the EU-GDPR as the central topic of interest, and their outcomes relate to a specific aspect of the regulation. They address five key themes: data protection rights, consent, transparency, accountability, and technical and organizational measures.
3. *Data privacy and security* (110 studies): These studies contribute to domains that are related to the EU-GDPR and data protection, such as other regulations, general privacy research, cybersecurity, information ethics, information disclosure, and data sharing. While they position the EU-GDPR as a motivating factor for their outcomes, they do not analyze the regulation.
4. *General IS research* (94 studies): These studies relate to a variety of other IS research areas and only mention the EU-GDPR to back up a specific, isolated argument.

Hence, despite the increasing interest for EU-GDPR, research is still at an early stage and only the contributions in the first and second categories (i.e., 16% of all the studies) can be considered to fully embrace the EU-GDPR topic. Interestingly, these studies address typical topic areas in Bélanger and Crossler's (2011) taxonomy for information privacy research and are classified accordingly in Table 1. The early EU-GDPR studies (published until 2018) fell within the domains of information privacy practices and information privacy technologies and tools. After the EU-GDPR entered into force, researchers broadened their scope and started to investigate the information privacy concerns and attitudes of individuals and specific stakeholder groups (e.g., software developers, researchers, and business executives). Comparing the state of research in 2018 with 2020, we observe the most significant uptake in studies focused on technologies and tools for EU-GDPR compliance, which now constitute the majority of EU-GDPR-related studies (i.e., 41% in 2020, up from 28% in 2018). Four of these studies (out of 16) investigate blockchain as a technological basis for compliance solutions. By contrast, studies on information privacy practices were predominant in 2018 (i.e., 57%) but now rank second after technology and tools-related research (i.e., down to 31% in 2020). They predominantly comprise empirical studies of EU-GDPR-related practices. Finally, the share of studies classified in the information privacy impact category has dropped slightly from 28% in 2018 to 20% in 2020. These studies investigate the impact of the EU-GDPR on emerging technologies (e.g., advanced analytics and smart products) and business model innovation, as well as the economic/market impact of data portability.

Table 1 also illustrates that research on the EU-GDPR is fragmented and many studies narrowly focus on one of the EU-GDPR's requirements and the technologies, tools, or practices used to address them. With respect to consent, these studies investigate, for example, the means to influence it on digital channels (Bergram et al., 2020) or whether existing implementations comply with the regulation (Kurtz et al., 2020). Several studies suggest blockchain-based solutions (Faber et al., 2020; Guggenmos et al., 2020; Mejtoft et al., 2019; Rieger et al., 2019) or enterprise architecture (Burmeister et al., 2019, 2020). These approaches have two shortcomings: First, most papers take the compliance requirements for granted and directly look into specific practices or solutions. They thereby do not take into account that the regulation remains abstract and does not prescribe nor endorses concrete implementation options, and that enterprises need to translate it and develop suitable data management practices supporting compliance. Second, these studies address isolated aspects of the regulation, that is, a single regulatory requirement or a limited set thereof, and suggest targeted solutions to address them. Hence, we still lack a broader and implementation-agnostic understanding of the compliance requirements and the ways to address them.

The 19 studies on the overall regulation mostly evaluate existing practices and concerns or analyze the EU-GDPR's impact on a specific domain (e.g., social media discourse, innovation, and Big Data). Yet, they fail to provide insights

into the entire regulation's implications from an enterprise-wide perspective. Russell et al. (2018) address this topic by proposing a digital-privacy transformation "gap-map" that would measure the organization's propensity for change. However, it exclusively takes a change management perspective without investigating the compliance requirements and their implications for enterprise data management.

Regulatory compliance management

So far, the academic discussion on the EU-GDPR has not connected with the regulatory compliance management (RCM) research domain, although the latter provides systematic approaches to analyzing regulations and their influence on business practice. Regulatory compliance management aims to "ensur[e] that enterprises are structured and behave in accordance with the regulations that apply, i.e., with the guidelines specified in the regulations" (El Kharbili, 2012). Regulatory compliance management introduces useful definitions to delineate relevant legal concepts: It distinguishes between regulations (i.e., binding document), regulatory guidelines, and compliance requirements, as provided in the legal text. After interpretation, this ultimately results in compliance requirements being implemented (El Kharbili, 2012). The so-called concretized compliance requirement describes the implementation of a CR in an enterprise context, fulfilling its legal specification.

Two papers from 2009 analyze the coverage of RCM in IS research. Cleven and Winter (2009) isolated 26 relevant papers and analyze them through the lens of enterprise architecture. They found that while some RCM aspects have been prominently studied (e.g., organizational and behavioral impacts of regulations, compliance-supporting IT solutions), others have been neglected. Specifically, they found no contributions on the operationalization of compliance objectives. The review by Abdullah et al. (2009) on RCM revolves around the approaches (i.e., explanatory or solution) and context (i.e., region, type, and domain) of the considered contributions. Most of the 45 papers concern North America, and only three of them focus on Europe. Regarding data protection, they identify two papers on Fair Information Practices and only one on the European Data Protection Directive (95/46 EC), even though it had been enforced for more than a decade. Furthermore, all identified contributions offer either preventive or detective solutions, but no corrective solutions. The authors hypothesize that corrective solutions are an outcome of legal analysis, which is why they were not addressed by the IS community.

Hence, there is a lack of RCM-related contributions that address data protection regulations, focus on regions other than North America (Abdullah et al., 2009), or provide guidance to achieve strategic compliance objectives (Cleven and Winter, 2009). This last call is echoed by our literature review on the EU-GDPR—although there have been contributions on the topic, they all focus on specific aspects of the regulation. Thus, we lack a single integrated framework for the EU-GDPR that takes an enterprise-wide perspective on the compliance requirements and analyzes ways to address them without prescribing specific implementation choices.

Research design

Context and research objectives

Our research activities were carried out in a multi-year research program on data management, which followed the consortium research method (Österle and Otto, 2010). This setup provides close collaboration between academics and experts from multinational organizations active in various industries[3] and detailed insights into EU-GDPR implementation initiatives. It follows the collaborative practice research tradition and aims to add to the knowledge of involved professional and scientific communities alike, in order to advance practices in the area of interest (Mathiassen, 2002).

Our research objective was to jointly develop prescriptive knowledge in terms of Gregor's (2006) type V theory that supports companies in achieving EU-GDPR compliance. Accordingly, we adopted design science research (DSR) as our central research paradigm to develop a capability model as an artifact "to solve identified organizational problems" (Hevner et al., 2004) relating to data protection—a highly interdisciplinary topic that is located at the intersection of legal practice and enterprise data management. Capability models are a type of reference models, which build on the RBV as underlying theory and outline the relevant set of capabilities that make up an organization's ability to "perform a set of coordinated tasks, utilizing organizational resources, for the purposes of achieving a particular end result" (Helfat and Peteraf, 2003). Reference models support the accumulation of knowledge, as they allow to explicate, integrate, and consolidate the fragmented knowledge that is available in the form of situational designs and emerging practices (vom Brocke and Buddendick, 2006). In enterprise data management, capability models have been suggested by academics and professionals to structure and assess data management practices, emphasizing the required capability-building from the deployment of different types of resources (Legner et al., 2020).

Research process

In order to develop the capability model with the due scientific rigor, we followed the research process outlined by Peffers et al. (2007). We initiated our research activities with a problem-based entry point, where objectives and solutions are not yet defined. Following the problem analysis, we developed the capability model in two main

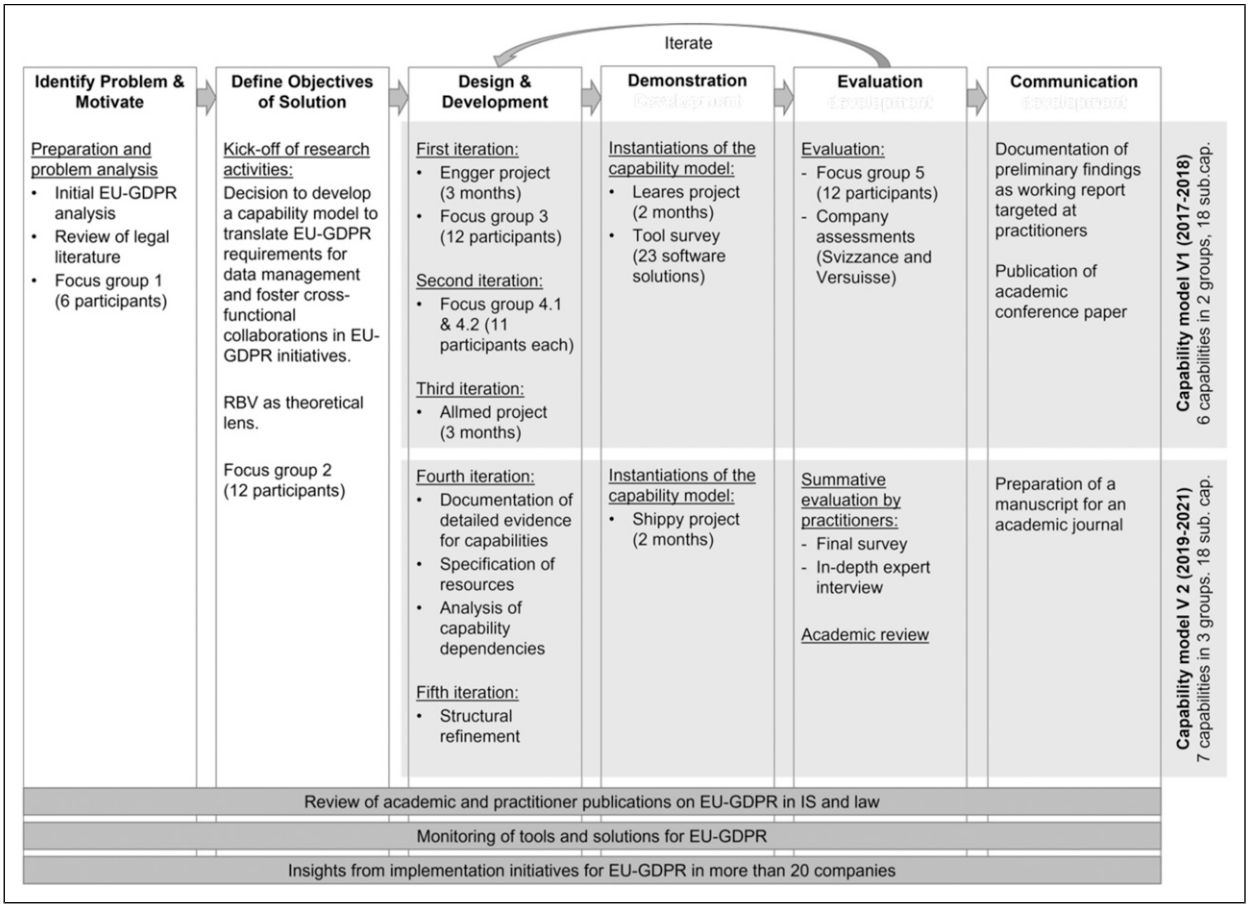

Figure 1. Research process with problem-centered initiation based on Peffers et al. (2007).

phases, each comprising iterative design cycles, as well as demonstration and evaluation steps. We will elaborate on the different steps of our research process in the next sections (see Figure 1 for the overview) and provide evidence on how the capability model developed along the two main phases. The iterative nature of the chosen design science research process allows for the integration of theoretical elements and practitioner feedback. Thus, throughout the research process, we used RBV concepts to theoretically ground and structure our insights from different types of research activities: an analysis of legal texts, official guidelines, and interpretations on the EU-GDPR, a review of EU-GDPR-related tools, and close interactions between academics and practitioners, comprising five focus group meetings with 33 data management experts from 22 companies, as well as insights from four EU-GDPR projects.

Problem identification and definition of objectives. Preparation for the research activities started in early 2017 and reflects the problem-centered initiation of our research process. These activities were meant to understand the problems that EU-GDPR implementation entails and specify the research objectives. In an initial review of the regulation, we extracted the EU-GDPR's compliance requirements and analyzed them according to foundational data protection principles in legal literature (i.e., personal data, informational self-determination, accountability, and transparency). Early results of this analysis were discussed with practitioners (focus groups 1 and 2) and revealed two main challenges regarding EU-GDPR compliance. First, while anticipating significant changes to the current way of storing and processing personal data on an enterprise-wide level, participants recognized that they lacked a comprehensive understanding of the regulation itself. Second, they cited a lack of common ground with legal departments. In their organizations, discussions around data protection and privacy regulations are often cut short due to a lack of common approaches and vocabulary, which blocks the identification of feasible and compliant solutions and hinders progress. This led to the research objective of defining a capability model for the EU-GDPR that assists data management professionals in understanding and implementing the regulation and collaborating with their colleagues in the legal departments.

Development of the capability model's first version. From 2017 to 2018, the first version of the capability model (V1) was developed in three iterations involving insights from field projects and parallel research activities to design the capability model, as well as focus groups to collect feedback and additional instantiations to demonstrate the model. At first, we analyzed regulatory requirements in terms of general capabilities that come into play for achieving compliance. Then, we collected field evidence and expert feedback to further refine the sub-capabilities and analyze implementation options with the required technological, human, or intangible resources.

The first design iteration comprised a project at Engger[4], a global engineering company, and resulted in the initial draft of the capability model, comprising four capabilities and 15 sub-capabilities. Engger had just started a large-scale project around EU-GDPR-compliant personal data aimed at harmonizing business partner data management in a highly distributed landscape with around 500 systems in different countries and subsidiaries. This project helped to get a better understanding of the issues and define capabilities related to the collection and distribution of personal data and consent. The draft version of the capability model was discussed with experts from other companies in focus group 3.

In the second iteration, two focus group meetings (i.e., 4.1 and 4.2) helped clarify the scope of the capability model. It was decided to set aside all security-related considerations and focus exclusively on data management capabilities. In focus group 4.1, the practitioners indicated that security is usually a distinct function and consulted, while the data management aspects were rarely addressed. From an academic perspective, information security is a well-research field, and the existing concepts may be translated to EU-GDPR, whereas there is little coverage of data management practices in regulatory compliance with data protection regulations. We also performed a re-mapping of the capabilities and grouped five capabilities and 17 sub-capabilities into two capability groups based on the demarcation between organizational and system capabilities found in RBV literature (Bharadwaj, 2000, Baiyere and Salmela, 2014).

The third iteration comprised a project around consent management at Allmed, a global pharmaceutical company. Its technical team had designed a minimum viable product solution, which we analyzed based on the capability model. Insights from the project together with a resulted in a stable set of six capabilities, with a new capability addressing data protection rights specifically, and 18 sub-capabilities, organized around two capability groups.

This capability model was subsequently demonstrated and evaluated: It was demonstrated with the EU-GDPR activities at Leares, a small consulting firm, where it proved to be a useful and efficient tool for assessing the current capabilities, identifying the required capabilities, and prioritizing compliance activities. In parallel, we used the capability model to analyze and classify 23 software tools from major vendors claiming to support EU-GDPR compliance (cf. Appendix 1, with tools falling into the common categories of data management, compliance and identity & access management (CIAM), security, and enhancement). This analysis allowed us to further validate that the identified capabilities and sub-capabilities were complete and exhaustive.

We then conducted additional expert interviews to evaluate the artifact's simplicity, understandability, fidelity, and completeness (evaluation criteria as suggested by Prat et al., 2015). We selected the data protection officer, as well as a data management specialist from two major insurance companies in Switzerland, Versuisse and Svizzance, which are among the country's Top 10 providers of life and non-life insurance and also operate in EU countries. Interviews consisted of a walkthrough of each capability to discuss and evaluate the company's standing and practices. At the end of each interview, we asked participants to rate the capability model's simplicity, understandability, and completeness using a five-point Likert scale (where 1 = fully disagree, 3 = neutral, and 5 = fully agree). Our respondents rated the capability model's simplicity, understandability, and completeness with a minimum of 4 out of 5. The fidelity dimension was the only one without a rating of 5, as respondents rated it with 3 and 4. Respondents with a legal education indicated that although the capabilities seemed to adequately reflect the EU-GDPR requirements, they were missing assignments of each capability to the regulation's principles. Similarly, data management expressed that although capabilities matched the requirements that they discussed with members of their organizations' legal teams, there was a lack of explicit reference to the regulation. Participants in focus group 5 confirmed those results.

Development of the capability model's second version. While the first version focused strongly on the practical relevance and utility, it had certain shortcomings in terms of documentation and was mainly built from experiences gained in early-stage initiatives. After the EU-GDPR went into effect, we observed an increase in academic studies and more open debates and testimonials from companies related to their implementation approaches and challenges. In 2019, we decided to launch a second phase that would allow us to validate and enhance the capability model based on the insights from the increasing number of EU-GDPR publications, while improving its theoretical grounding. From 2019 to 2021, we conducted two additional design iterations, with subsequent demonstration and summative evaluation, resulting in the second and final version of the capability model (V2).

In parallel, we continued to analyze EU-GDPR-specific legal literature to inform the development of the capability

model, ensuring a proper fit with legal requirements. For this purpose, we gathered and analyzed material from authoritative data protection sources, such as textbooks from multiple legal traditions, for example, pan-European (European Union Agency for Fundamental Rights et al., 2018; Synodinou et al., 2017, 2021, 2020; Voigt and Von Dem Bussche, 2017), French (Bensoussan et al., 2018), Belgian (Docquir, 2018), and Swiss (Meier, 2011), as well as two recent doctoral dissertations (Staiger, 2017; Thélisson, 2020). We complemented this understanding with insights from official guidelines and interpretations from supervisory authorities (e.g., Chatellier et al., 2019; Commission Nationale de l'Informatique et des Libertés, n.d.; European Data Protection Board, 2017, 2018a, 2018b; European Data Protection Supervisor, 2018, 2019; Information Commissioner's Office, 2017), as well as academic papers and doctrinal opinions (e.g., Armingaud and Ligot, 2019; Castets-Renard, 2019; Cheffert, 2018; De Hert and Malgieri, 2018; De Hert and Papakonstantinou, 2012, 2016; Debet, 2018; Fellous-Sigrist, 2018; Groos and Veen, 2020; Hoeren and Kolany-Raiser, 2018; Karjoth and Langheinrich, 2019; Lazaro and Le Métayer, 2015; Naftalski, 2018; Puyraimond, 2019; Rallet et al., 2015; Solove, 2013; Wiese Schartum, 2018; Zanfir, 2014).

In the fourth iteration, we revised the capability model in light of expert feedback and the latest academic and practitioner literature. We monitored EU-GDPR-related studies until Q4 2020, updated the literature review, and integrated insights from selected publications as support for relevant capabilities and the resources deployed in different implementation options. To improve the documentation's consistency and completeness, we mapped each capability, sub-capability, and software features with relevant EU-GDPR recitals and articles. The combination of practitioner and research insights also enabled us to specify relationships and dependencies between capabilities and isolate enabling ones. This iteration entailed a project at Shippy, a European shipping company, where the model was applied by a consultant that had not been involved in its development.

In the fifth iteration, we integrated academic feedback and reassessed the capability model's structure based on the existing theoretical framework on IT capabilities. Specifically, we mapped capabilities and sub-capabilities to prominent RBV-based categorizations (following Bharadwaj et al., 1999, and Wade and Hulland, 2004) in order to accurately reflect their characteristics and theoretical underpinnings. Based on this analysis, we combined the capabilities and sub-capabilities dealing with the relationships with external entities and added a dedicated capability group, resulting in three capability groups (with seven capabilities and 18 sub-capabilities).

Finally, we conducted a summative, two-pronged evaluation consisting of an evaluation questionnaire presented to practitioners after a capstone presentation on the research project, as well as a debriefing session to analyze lessons learned from the Shippy project. Through the questionnaire, we evaluated the capability model's understandability, completeness, consistency, simplicity, usefulness, and applicability by using the same five-point Likert scale as in the first evaluation. All dimensions received ratings of 4 and above, except for simplicity and applicability, which one of the respondents rated as "neutral" (3 points). The debriefing of the Shippy project confirmed that the capability model creates common ground between legal and data management practice and helps data experts understand the regulation (quotations from the interview can be found in Appendix 3). Regarding the model's ability to support (i) assessments and roadmap planning, (ii) progress monitoring, and (iii) communication and change management, all dimensions received a minimum rating of 4 (on four counts), and the majority received a rating of 5 (on six counts).

Data management capabilities for the EU-GDPR

Capability model: Theoretical foundations

According to EU-GDPR art. 24 § 1, an organization is responsible for implementing "appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with this Regulation." Using the RBV as theoretical lens, we argue that achieving compliance with EU-GDPR at an enterprise level requires building dedicated capabilities for processing and storing personal data. Capabilities are "complex patterns of coordination between people and between people and other resources" (Grant, 1991) that are embedded in organizational practices and individual skills (Bharadwaj et al., 1999). In the data protection domain, building these capabilities requires an organization to deploy three types of resources in predictable patterns of activity (Barney, 2001, Bharadwaj et al., 1999):

- *Human resources* taking over relevant roles for data protection, for example, a data protection officer, a contact person for data rights requests, or an enterprise data architect.
- *Technological resources* comprising physical IT assets (hardware, software, and databases) that enable data protection compliance, for example, a data processing system, a dedicated consent-management tool, and a self-service portal for data rights requests.
- *Intangible resources* representing the data protection-related know how, for example, frameworks, standards, process models, as well as data and enterprise architecture documentation.

While the RBV considers firm performance through sustainable competitive advantage (Barney, 1991) as the goal of capabilities (the why), we argue that capabilities for data protection are built with a regulatory compliance objective or, as conceptualized by Sadiq et al. (2007), to reach an organization's "control objectives" (see Figure 2). As the business impact of compliance activities is hard to quantify in financial terms, they are seldom cited as a source of competitive advantage. However, non-compliance may have significant direct (e.g., fines) and indirect (e.g., reputation loss) impact on a company's ability to generate profit, thus impacting its performance. This is also supported by IS studies that have investigated the links between governance and compliance on the one hand, and business value and organizational success on the other hand (Buchwald et al., 2014; Heier et al., 2007; Ritschel et al., 2005). Hence, we argue that such "control objectives" can be viewed alongside competitive advantages as components of firm performance. Therefore, based on Zhang et al.'s (2013) definition of an IT capability, we define data management capabilities for regulatory compliance as *a firm's ability to acquire, deploy, and leverage its technological, human, and intangible resources in combination with other resources and capabilities to achieve an organization's*

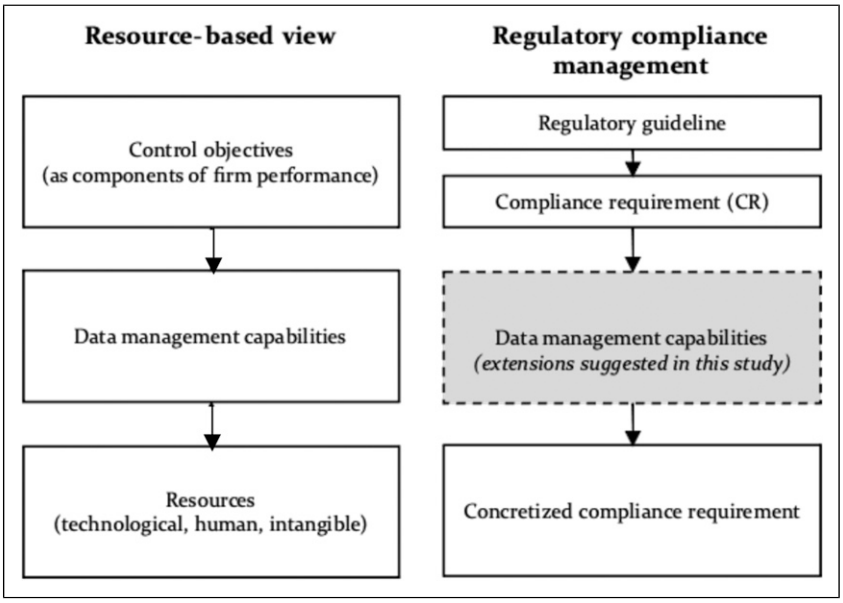

Figure 2. Data management capabilities for regulatory compliance from the lens of RBV and RCM.

Table 2. Capabilities as link between compliance requirements and their concretization.

RCM concept	Definition (based on El Kharbili, 2012)	Illustration in EU-GDPR
Regulatory guideline	Stipulates a set of obligations to comply with.	Art. 6—"Lawfulness of processing": enumerates conditions in which data processing is legal.
Compliance requirement (CR)	Pieces of text extracted from the regulatory guideline specifying an expected behavior or a specific condition to fulfill.	Extraction of requirements bearing data management relevance. For example, art. 6 § 1 a and art. 7 § 1 require that data be processed according to individuals' expressed consent.
*Data management capabilities**	*Result of the interpretation of CRs in terms of capabilities that are to be implemented or improved.*	*Manage consent and sub-capabilities: implement consent items, collect consent instances, distribute consent, enforce consent-based processing.*
Concretized compliance requirement (CCR)	Implementation of a CR in an enterprise context, fulfilling its legal specification, by a concrete set of technological, human and intangible resources.	A concrete measure is implemented in a specific organization to operationalize CRs. For example, "In company X, existing IS resources, such as a CRM system, must be configured so that consent data is first recorded in system 1 and pushed to other systems every 12 hours."

*extension suggested in this study.

Table 3. Capability model for EU-GDPR.

(A) Infrastructure Capabilities				
(A1) Protected data scope definition	(A1.1) Identify data objects	(A1.2) Classify data attributes	(A1.3) Locate data records	
(A2) Consent processing	(A2.1) Implement items of consent	(A2.2) Collect instances of consent	(A2.3) Distribute consent	(A2.4) Enforce consent-based processing
(A3) Personal data removal	(A3.1) Delete data	(A3.2) Pseudonymize data		
(B) Management Capabilities				
(B1) Data protection orchestration	(B1.1) Assume data protection responsibilities	(B1.2) Oversee data protection activities		
(B2) Data protection evaluation and control	(B2.1) Maintain records of processing activities	(B2.2) Maintain documentation of system landscape	(B2.3) Supervise sensitive processing activities	
(C) External Linkages				
(C1) Data protection communication	(C1.1) Disclose information to individuals	(C1.2) Transmit data in standardized form		
(C2) Compliant processing demonstration	(C2.1) Control compliance of external processors	(C2.2) Cooperate with authorities		

control objectives related to the relevant data protection regulations.

The RBV also helps extending RCM concepts (El Kharbili, 2012) for the new generation of data protection regulations: Capabilities connect the normative aspects of the regulation (i.e., the regulatory guidelines and compliance requirements or CRs) and the concretized compliance requirements (CCRs), that is, the concrete implementation of a CR using technological, human and intangible resources. Table 2 depicts this connection and illustrates it for the EU-GDPR. The addition of data management capabilities to existing RCM concepts qualifies the interpretation of CRs and enables their translation into what organizations should do (i.e., the capabilities) as opposed to how they should do it (i.e., the specific resources implemented and used for achieving compliance with the regulation). In doing so, capabilities create "common ground" between legal and IS perspectives and help analyzing compliance requirements in terms of changes to the existing routines and practices before a decision is made on concrete (technical) implementations.

Capability model: Structure and overview

Building on these foundations, we derived the capability model from EU-GDPR's underlying principles, as described in the legal literature, as compliance requirements. The capability model (see Table 3) comprises 7 capabilities, which reflect the "pillars" of the regulation, and 18 sub-capabilities, which were iteratively developed in our research process and integrate academic and practitioner knowledge. The EU-GDPR-related capabilities were grouped in three main capability groups based on the reference capability conceptualization of Bharadwaj et al. (1999) and Wade and Hulland (2004). Consequently, *Infrastructure Capabilities* are mainly concerned with the ability to implement the new data-related rights and consent-based processing in the data processing systems, *Management Capabilities* predominantly ensure EU-GDPR's accountability requirements (although they can still be supported by tools), and *External Linkages* capabilities relate to interactions and collaborations with entities outside the organization (e.g., data subjects, authorities, and other organizations).

In the following sections, we present each of the identified capabilities, along with the compliance requirements, the empirical insights from focus groups and projects, and the sub-capabilities. We also graphically depict the dependencies with other sub-capabilities (see Figures 3–10) and discuss the required resources for their implementation. For each capability, we also provide a synthesis (in Tables 4–10) with details about the sub-capabilities, their specification, implementation options (with exemplary resources) and the relevant compliance requirements (CR, extracted from the regulation).

Infrastructure capabilities

This capability group comprises three capabilities that ensure that data processing systems and architecture comply, in particular, with new data-related rights and the increased focus on consent-based processing in EU-GDPR.

Protected data scope definition (A1). This capability is based on art. 1 § 1 and 4 § 1 and denotes the ability to clearly identify, classify, and locate personal data. Personal data is defined as "data enabling direct or indirect identification of a single physical person, data that is specific to a single physical person without enabling identification, data that can be linked to a physical person, data regarding which anonymization techniques cannot completely mitigate the risk of re-identification".

Generally, companies faced two main challenges: determining what kind of personal data they were processing and where such data was stored. Focus groups 1 and 2 indicated that before the implementation of EU-GDPR, companies had had little to no real overview of the personal data they collected and used, especially in terms of storage location. A participant in focus group 4.2 asked: "How do

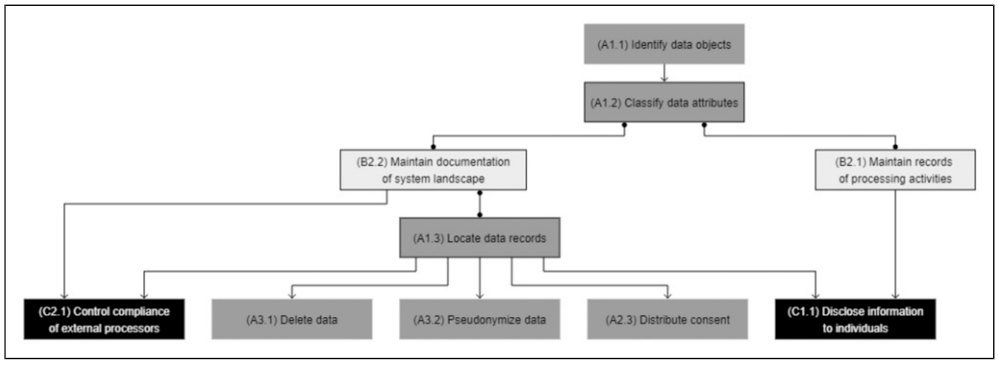

Figure 3. Capability relationships: Protected data scope definition (A1).[5]

Table 4. Capability overview: Protected data scope definition (A1).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Identify data objects (A1.1)	Ability to make a list of data objects that fall under the scope of the EU-GDPR in enterprise systems	Identify relevant data domains that contain personal data (e.g., customer, business partner, employee, and job applicant) Distinguish between identifying data (i.e., that can be linked to a specific individual) and non-identifying data (i.e., that cannot be linked to a specific individual)	Data crawlers with machine learning for personal data retrieval and identification (T) Documentation: enterprise architecture models, data models, application inventory, or data catalog (I) Manual scanning of applications and databases (H)	Art. 2 § 1 Art. 4 § 1 Art. 15 R. 26, 27, 30, 57
Classify data attributes (A1.2)	Ability to assign levels of data sensitivity to identify data attributes	Personal data (e.g., identity, contact, personal history, financial, and location, content) Sensitive data (e.g., opinions, health, biometry, ethnic origin, and criminal history) Data relating to children	Data crawlers with machine learning for personal data retrieval and classification (T) Documentation: enterprise architecture models, data models, application inventory, or data catalog (I) Manual scanning of applications and databases (H)	Art. 4 Art. 8-10 R. 34, 35, 38, 51
Locate data records (A1.3)	Ability to retrieve personal data objects from all relevant processing systems	Internal location (systems, storage media, responsible organizational unit) External location (third-party processors, geographic location)	Automated queries (T) Manual identification based on system landscape documentation (H) Documentation of data flows and data lineage (I)	Art. 4 Art. 15 Art. 28 R. 101, 103, 107, 108, 110

*Technological – T / Human – H / Intangible – I.

you identify personal data in a heterogeneous IT system landscape?", which led to a follow-up discussion around the means to identify personal data. In the project at Engger, one of the main objectives was to make sure that personal data was consistently kept up-to-date within all customer-facing websites and portals, which proved difficult due to multiple overlapping systems managed in independent subsidiaries.

The resulting capability may be best summarized by Bensoussan et al. (2018): "organizations must have perfect knowledge of personal data." Iannopollo et al. (2017) recommend two actions that mirror these issues (i.e., data inventory and system mapping) and suggest that personal data should be not only identified but also classified. This is required as the EU-GDPR prescribes higher levels of protection for data that is considered sensitive (R. 51). The resulting sub-capabilities are:

- *Identify data objects (A1.1):* ability to make a list of data objects that fall under the scope of the EU-GDPR in enterprise systems (e.g., customer, employee, or job applicant).
- *Classify data attributes (A1.2):* ability to assign levels of data sensitivity to identify data attributes within personal data objects.
- *Locate data records (A1.3):* ability to retrieve personal data objects from all relevant processing systems.

In terms of implementation, this capability is well aligned with the functional scopes of solutions in the data management and security/protection tool categories, as most of them provide functionalities supporting data discovery (i.e., retrieving data across the organization's entire system landscape) and classification (e.g., by using data crawlers). Practitioner insights indicate that building this capability is intertwined with intangible resources and creates significant effort for enterprise-wide documentation and classification activities. Svizzance and Versuisse, for example, were in the process of re-aligning existing data and system landscape documentation with their existing databases and systems by specifying additional details and updating them when necessary. For this purpose, both organizations turned to enterprise architecture tools to define and document the protected data scope—an approach that has also been proposed by academic research (Burmeister et al., 2019, 2020; Huth, Burmeister, et al., 2020). In the case of Leares, the company did not have any similar existing documentation, and it became clear that this capability should be the focus of initial efforts, as other capabilities could not be realized without understanding the protected data scope.

This capability can be viewed as a prerequisite to the two other infrastructure capabilities—that is, consent processing (A2) and personal data removal (A3), which require performing operations on previously identified data records. For instance, it is not possible to delete a data object if it has not been discovered and indexed.

Consent processing (A2). This capability comprises the prerequisites for collecting consent and ensuring the consent-based processing of information. The principle of consent (art. 7, Bensoussan et al., 2018; Nicolaidou and Georgiades, 2017; Voigt and Von Dem Bussche, 2017) is arguably one of the pivotal concepts of the EU-GDPR and an expression of the right to informational self-determination. It can be defined as each individual having the ability to determine whether and to what end information about themselves can be processed (Mitrou, 2017). The related concepts of conditionality, granularity, and specificity are the most challenging for data management (European Data Protection Board, 2018b) if compared with practices before the EU-GDPR, when consent was mostly obtained through the bulk acceptance of general conditions. Conditionality (art. 7 § 4) means consent for processing activities cannot be bundled into general conditions, and a difference should be made between necessary and optional processing activities for a given purpose. Granularity (R. 43)

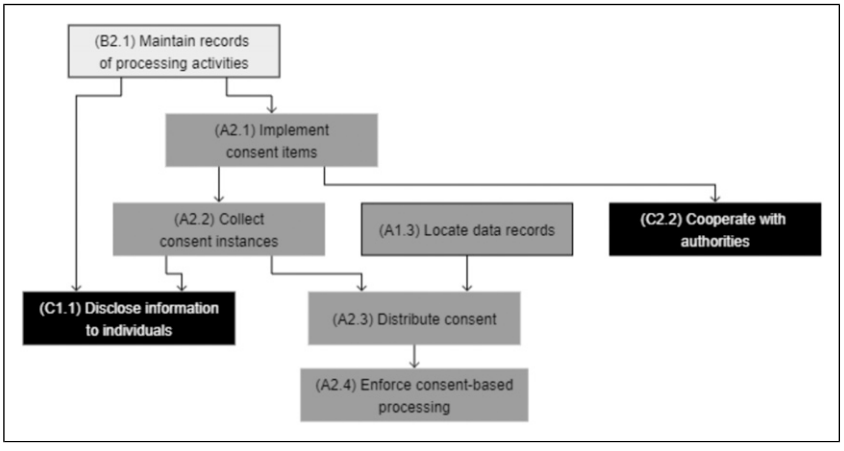

Figure 4. Capability relationships: Consent processing (A2).

Table 5. Capability overview: Consent processing (A2).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Implement consent items (A2.1)	Ability to define and implement consent items that mirror data processing activities performed by business entities	Define consent items (i.e., yes/no questions reflecting processing purposes that require explicit consent) Translate consent items into machine-readable data attributes	Addition of attributes in data (T) Metadata documentation (I) Consent management tool (T)	Art. 5-7 R. 33, R. 50
Collect consent instances (A2.2)	Ability to collect and record consent from data subjects	Enable individuals to provide consent for specific processing types and to change it (e.g., by adding new, modifying, or withdrawing existing ones)	Self-service portal (T) Request-based process (I) Consent management tool (T)	Art. 5-7 R. 32, 42
Distribute consent (A2.3)	Ability to keep consent instances updated throughout all impacted systems	Changes of consent recorded in one system should be propagated within all other systems containing personal data about the targeted individual	Centralized repository (T) Data integration platform (T)	Art. 5-7
Enforce consent-based processing (A2.4)	Ability to control (i.e., enable or restrict) data processing activities on the basis of consent items	Ensure that consent items are actually taken into account throughout all business processes	Metadata attributes readable by processing systems (T) Data catalogs (T) Authorization and access control (I)	Art. 5-7 R. 40, 42

*Technological – T / Human – H / Intangible – I.

implies that each processing activity and related consent item must be presented separately. Specificity prescribes a 1:1 relationship between processing types and consent items (i.e., yes/no question that relates to a personal data processing activity).

Consent management greatly resonated among the experts in our focus groups and was a key concern in the Allmed project. During focus group 4.1, none of the participants reported solutions either in the final or the operational stages. During focus group 4.2, more questions were asked regarding consent management than all the other capabilities combined. The goal of the Allmed project was to make consent-related information accessible and readable by all the systems and, thus, mirror the "distribute consent" and "enforce consent-based processing" sub-capabilities. However, difficulties arose in two areas. First, the system would need to be connected to every system storing and processing personal data. However, identifying such systems proved difficult, and the existing system landscape documentation was deemed insufficient (see the capability "define protected data scope"). Second, the team struggled to identify consent items, as they were usually contained in an unstructured format (e.g., within general conditions, contracts, and webpages). A specific sub-capability was added to reflect this issue as a prerequisite to all other consent-related capabilities. The resulting sub-capabilities are:

- *Implement consent items (A2.1):* ability to define and implement consent items that mirror data processing activities performed by business entities.
- *Collect consent instances (A2.2):* ability to collect and record consent from data subjects.
- *Distribute consent (A2.3):* ability to keep consent instances updated throughout all impacted systems.
- *Enforce consent-based processing (A2.4):* ability to control (i.e., enable or restrict) data processing activities on the basis of consent items.

This capability relies mainly on new or augmented technological resources. While the concept of consent itself was not new, the granularity requirements introduced by the EU-GDPR posed a significant technical challenge in the existing system landscapes. They imply that additional data reflecting consent must be collected and taken into account when processing the related data objects in both manual and automated processing scenarios. From a tool perspective, data management, compliance management, and access management solutions offer specific modules to record user consent, especially in scenarios involving a web-based frontend. However, even though such tools provide the technical means to communicate and acquire consent, organizations still face the issues of defining and implementing consent items (A2.1). In that regard, the

difficulties encountered by Allmed's team in defining what items should be recorded once again highlight that technical implementations are dependent on the transparency regarding processing activities. This difficulty is also found in the study by Kurtz, Wittner, et al. (2020), which identifies 18 problems related to gathering consent on the eBay platform and highlights gaps between stated and effective processing purposes in digital service offerings. Huth, Both, et al. (2020) also explore the necessity for technical and development teams to recognize consent items and subsequently investigate implementation modalities. They suggest a prototype to support related discussions between development and business teams in the context of agile software engineering. Both studies suggest that consent requirements, due to their impact on final designs, should be integrated during early stages of IT development, which can explain the difficulties in bringing pre-existing solutions to compliance.

Personal data removal (A3). This capability denotes the ability to process data according to the EU-GDPR's data rights and principles. It was derived from the principle of accountability (art. 24 § 1) but covers only the technical aspects to reach compliance, document them, and provide proof of compliance (Bensoussan et al., 2018; Nicolaidou and Georgiades, 2017; Voigt and Von Dem Bussche, 2017).

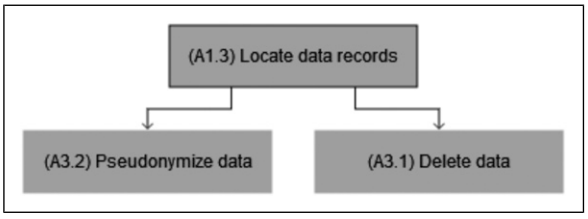

Figure 5. Capability relationships: Personal data removal (A3).

Art. 17 provides for a right of erasure ("right to be forgotten"), according to which individuals can request that organizations delete their personal data (provided that they have no other obligation to keep said data). Prior to the EU-GDPR, enterprise systems usually prevented users from deleting data, and practitioners expressed frustration in this regard. When asked about it, none of the participants of focus group 4.1 reported that they had operational deletion processes or mechanisms in place, and participants expressed a lack of well-established solutions at this level. Art. 25 mandates privacy by design or by default approaches, including the principle of minimization (Voigt and Von Dem Bussche, 2017), that is, processing as little personal data as possible. One way of operationalizing it is through pseudonymization, which is a rare occurrence of EU-GDPR mentioning a specific technological approach (R. 28-29). Pseudonymization or anonymization is a form of data processing—in that sense, while they may, for instance, enable organizations to lighten the privacy assessment requirements or to use a legal basis other than consent, processing of anonymized/pseudonymized data should still have a legal basis and does not relieve organizations of all data protection responsibilities (Groos and Veen, 2020). For this reason, pseudonymization was added, which resulted in two sub-capabilities:

- *Delete data (A3.1):* ability to permanently remove data records.
- *Pseudonymize data (A3.2):* ability to process personal data in a way that they cannot be linked to a specific individual.

Table 6. Capability overview: Personal data removal (A3).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Delete data (A3.1)	Ability to permanently remove data records	Deletion of all storage instances of data objects/attributes should be carried out if they no longer serve a purpose, or upon request, pending other legal obligations	Deletion functionality (T) Automated deletion processes (T) Blockchain (Farshid et al., 2019) (T)	Art. 17 R. 65, 66
Pseudonymize data (A3.2)	Ability to process personal data in a way that it cannot be linked to a specific individual	Data that is pseudonymized (e.g., stripped of any link to a specific individual) does not fall into the scope of the EU-GDPR, provided this process is not reversible. In case of reversibility, information-enabling linkages to individuals must be kept outside the organization by a trusted third party Pseudonymization should be used whenever possible	Cryptography tools (T) Hash functions (T)	Art. 4 § 5 Art. 5 § 1(c) Art. 11 Art. 25 R. 28, 29, 78

*Technological – T / Human – H / Intangible – I.

Building this capability relies heavily on technological resources, but features related to data deletion seem to be the least frequent—they were only enabled by two solutions in our tool study, and only one of them supported the enforcement of a data retention policy. Data anonymization and data pseudonymization are also rather uncommon because encryption mechanisms, which are generally already in use for security purposes, seem to be favored. Furthermore, unless the keys are kept by a trusted third party, symmetrical encryption is not a valid means for data pseudonymization as it can be reversed. These shortcomings are confirmed by research, and several studies have investigated blockchain as a technological foundation for the design of systems that enable true pseudonymization (Faber et al., 2020; Farshid et al., 2019; Guggenmos et al., 2020; Mejtoft et al., 2019; Rieger et al., 2019).

Management capabilities

This capability group comprises two capabilities that enable the organization to comply, in particular, with EU-GDPR's accountability requirements.

Data protection orchestration (B1). This capability denotes the organizational ability to coordinate and execute data protection activities involving different roles and responsibilities. It was derived from the organizational component of the principle of accountability (Bensoussan et al., 2018; Nicolaidou and Georgiades, 2017; Voigt and Von Dem Bussche, 2017). As stated, focus group feedback indicated that data managers are often at a loss as to whom they can consult when faced with data protection inquiries. This became particularly clear during the Allmed project, when the team needed to obtain information regarding data protection matters but struggled on several occasions because responsibilities (e.g., defining consent items) were not clearly defined. Art. 37-39 requires that organizations of a certain size appoint a "data protection officer" (DPO). The DPOs should monitor compliance by getting an overview of processing activities, serve as advisory contact person (European Data Protection Board, 2017), oversee record keeping, and cooperate with authorities.

The resulting sub-capabilities are:

- *Assume data protection responsibilities (B1.1):* ability to establish data protection responsibilities in business functions that process personal data.
- *Oversee data protection activities (B1.2):* ability to oversee, organize, control, and coordinate data protection activities.

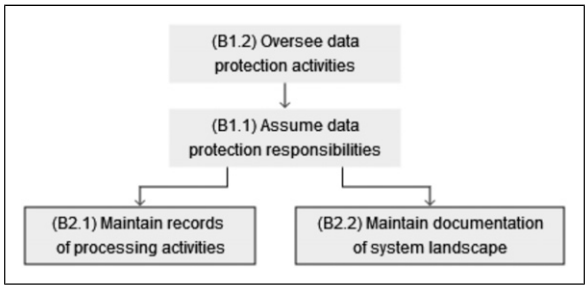

Figure 6. Capability relationships: Data protection orchestration (B1).

Building this capability requires companies to focus on the human resources taking over relevant roles for data protection on legal, IT, data management, and business sides. The DPO is a role that already existed in some organizations (e.g., "privacy officer") before the EU-GDPR and has been made mandatory by the regulation. However, even though the responsibilities are generally described in the regulation, the specificities remain unclear. In their recent EU-GDPR readiness study, Dansac Le Clerc and Mannent (2020) find that most DPOs have a legal background (62%), and only 21% of them are experts in IT/digital domains. They also

Table 7. Capability overview: Data protection orchestration (B1).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Assume data protection responsibilities (B1.1)	Ability to establish data protection responsibilities in business functions	Each business function should have people: (1) acting as the main contacts for data protection matters (2) carrying out data protection–related processes and providing input for data protection tasks	Roles and responsibilities (H) Company-wide directory of data protection stakeholders (I) Collaborative/ communication platforms (T)	Art. 26-28 Art. 37-39 R. 74
Oversee data protection activities (B1.2)	Ability to oversee, organize, control, and coordinate data protection activities	Role entailing advisory function, control, and cooperation with authorities	Data protection officer (overarching, coordination role) (H)	Art. 31 Art. 37-39 R. 48, 97

*Technological – T / Human – H / Intangible – I.

report that DPOs "have less experience in IT and security than they judge necessary." This corroborates statements from representatives of Versuisse and Svizzance, where DPOs were both coming from legal teams. Dansac Le Clerc and Mannent (2020) also highlight that EU-GDPR-oriented efforts should involve a "chain of compliance and responsibilities," extending beyond legal teams toward IT, security, HR, and business units. At Svizzance, the DPO reached out to the data management team and formed a partnership with one team member, who acts as a technical advisor to the DPO and coordinates decisions with the data management team. One of the outcomes of this partnership was a decision to refine existing enterprise architecture documentations of systems and processes in light of data protection requirements. Huth, Burmeister, et al. (2020) analyzed the collaboration between enterprise architecture and data protection teams and found evidence that using enterprise architecture as a basis for joint documentation was a successful course of action. In addition, tools from the data management, compliance management, and security/protection categories can also assist organizations in defining governance and centralizing workflows and policies. Implementing key performance indicators related to data protection activities from content (e.g., proportion of data protection–related fields actually maintained in databases) or process (e.g., frequency of updates of documentation) perspectives may also be considered to keep track of compliance activities.

Data protection evaluation and control (B2). This capability comprises the ability to record and evaluate sensitive processing activities, as well as document system landscapes. It was derived from the documentation component of the principle of accountability (Nicolaidou and Georgiades, 2017; Voigt and Von Dem Bussche, 2017). Art. 30 orders organizations to "maintain a record of processing activities under its responsibility" and details the contents of such documentation. It was identified as a significant difficulty by Iannopollo et al. (2018), and all the participants of focus group 4.2 acknowledged that documentation represented a significant effort. Besides recording processing activities, maintaining system landscape documentation was identified as another sub-capability, as the experts indicate that most organizations have difficulties locating data given the large number of systems—this was the very motivation for the Engger project and a significant roadblock for Allmed's solution implementation. Art. 35 and 36 further require organizations to conduct and document in-depth data protection impact assessments (DPIAs) when performing sensitive processing activities. The resulting sub-capabilities are:

- *Maintain records of processing activities (B2.1):* ability to create a list of and document personal data-related activities.
- *Maintain documentation of system landscape (B2.2):* ability to create a list of and document systems storing and processing personal data.
- *Supervise sensitive processing activities (B2.3):* ability to assess and document the privacy-related consequences of sensitive processing activities in detail.

Building this capability relies on intangible resources that are the basis for the ongoing recording of data processing activities. Documenting the systems that store and process personal data, as well as for processing purposes, is a pillar of EU-GDPR compliance and highly interdependent with the sub-capabilities for defining the protected data scope (A1). In terms of technological resources, solutions offer functionalities that can support and streamline the documentation process. Tools from most categories offer functionalities to detect irregularities in data use and detect data breaches, with tools in the protection/security category taking the lead. While the majority of surveyed solutions offer logging capabilities, which can prove useful to investigating suspected or known incidents, only three of them assist organizations in running DPIAs. This is partly because DPIAs are about interpreting the purpose of specific processing activities and evaluating potentially nefarious real-world consequences for individuals. Researchers have highlighted the need to refine

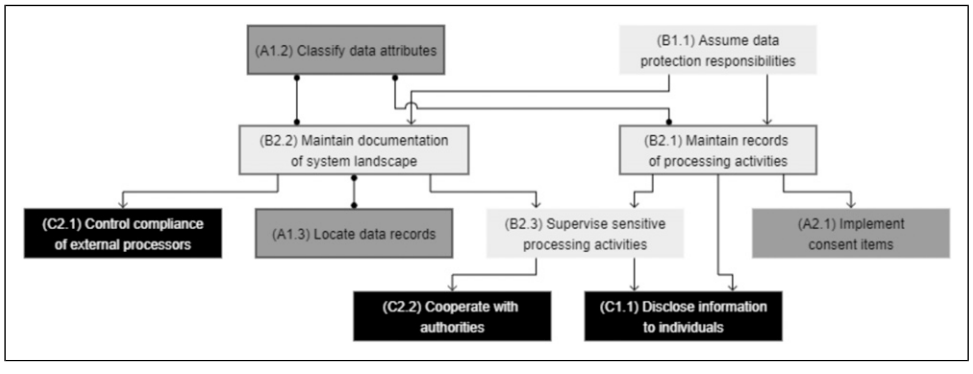

Figure 7. Capability relationships: Data protection evaluation and control (B2).

Table 8. Capability overview: Data protection evaluation and control (B2).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Maintain records of processing activities (B2.1)	Ability to create a list of and document personal data-related activities	Create a list of and describe all processing activities in terms of: basis of processing, data used, purpose, means (e.g., use of analytics), consent items requested	Enterprise architecture (I) Documentation templates (I) Process maps (I) Data flows/lineage (I) Documentation and review processes (H)	Art. 25 Art. 30 R. 39, 44-50, 78
Maintain documentation of system landscape (B2.2)	Ability to create a list of and document systems storing and processing personal data	Create a list of and describe all systems processing personal data in terms of stored data types and processing capabilities	Enterprise architecture (I) Documentation templates (I) Enterprise architecture tools/ maps (I) Documentation and review processes (H)	Art. 30
Supervise sensitive processing activities (B2.3)	Ability to assess and document the privacy-related consequences of sensitive processing activities in detail	Required when the scale of processing and/or the sensitivity of data processed or technology used pose high risks to privacy (e.g., advanced analytics, profiling) Subjected to specific authorization if satisfactory privacy measures cannot be implemented	Documentation templates (I) Review processes (I/H)	Art. 35 Art. 36 R. 51-56, 84, 90-92, 94

*Technological – T / Human – H / Intangible – I.

currently available methods and further investigate tool implementation (Vemou and Karyda, 2018). Another aspect involves the sensitivity of certain processing activities due to their novel technological underpinnings. There is an ongoing debate over the data protection–related risks of technologies such as Big Data Analytics and Artificial Intelligence (Addis and Kutar, 2020, 2018), and EU-GDPR specifically considers decisions that are the result of automated decision-making processes (art. 22). Conversely, researchers are investigating ways to incorporate ethics and transparency considerations into the design of Big Data artifacts and algorithms (Tona et al., 2018; Watson and Nations, 2019).

External linkages

This capability group comprises two "outside-in" capabilities according to Wade and Hulland's (2004) typology, that enable the organization to manage the relevant external relationships with data subjects and authorities and comply, in particular, with EU-GDPR's information, notification and cooperation requirements.

External data communication (C1). This capability involves the ability to disclose information to individuals (R. 58) and denotes the ability to process data according to EU-GDPR's requirements when processing activities entail data transmission to other third-party actors. It was derived from the principles of transparency, which requests that data protection measures be clearly presented, as well as the principles of accountability (art. 24 §1) (Bensoussan et al., 2018; Nicolaidou and Georgiades, 2017).

Transparency requirements apply in two cases (European Data Protection Board, 2018a). First, at the point of data collection, organizations must present related information separately in an easily comprehensible manner (e.g., language and illustrations). Transparency also refers to communications with individuals after data is collected, when organizations are faced with right-related requests (e.g., access, rectification, and deletion). The resulting sub-capability is:

- *Disclose information to individuals (C1.1):* ability to respond to data protection–related requests from data subjects and communicate data processing activities in clear terms.

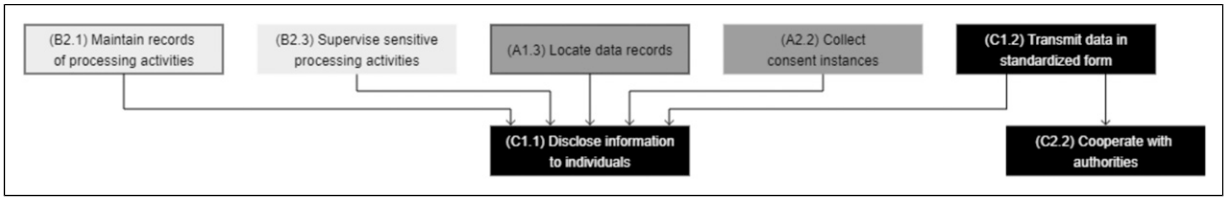

Figure 8. Capability relationships: External data communication (C1).

Table 9. Capability overview: External data communication (C1).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Disclose information to individuals (C1.1)	Ability to respond to data protection–related requests from data subjects and communicate data processing activities in clear terms	Data records must be disclosed to data subjects in the exercise of the following rights: access, rectification, portability, and deletion Information about processing activities and consent items must be presented in clear, everyday language, separately from other terms and agreements Data breach notification	Self-service portal (T) Request-based approach and processes (I/H) Contact person for individuals (H) Incident response processes (I/H)	Art. 12-23 Art. 34 Art. 36 Art. 38 § 4 R. 39, 58-73, 86
Transmit data in standardized form (C1.2)	Ability to transmit data to third parties using free and/or interoperable formats and to set up communication channels with other organizations	*Right of access*: communicate a complete list of data records in a freely readable format/ media *Right of portability*: communicate data records in a machine-readable way (to the individual or directly to a designated third party)	*Right of access*: PDF, OpenDocument (T) *Right of portability*: XML-based formats (+ dedicated communication channels if applicable) (T) Blockchain (Faber et al., 2020) (T)	Art. 15 Art. 20 R. 59, 68

*Technological – T / Human – H / Intangible – I.

This sub-capability is about presenting all relevant information regarding an organization's data protection practices at the time of data collection and at any point during data processing. It may be viewed as the operationalization of the principle of accountability, which is materialized through documentation and streamlined request processing.

Extending individual rights, art. 20 introduces a "right to data portability." Organizations are required to transmit personal data records "in a structured, commonly used and machine-readable format" to individuals and, in some cases, directly to other organizations. Researchers have highlighted that facilitating customer movement between (competing) organizations is a prime example of conflicting interests between compliance and business mandates (Engels, 2016; Wohlfarth, 2019). From a technical standpoint, during focus group 4.1, only a quarter of respondents declared that the provision of data in standardized formats was mature, and none of them reported working communication channels. The resulting sub-capability is:

- *Transmit data in standardized form (C1.2):* ability to transmit data to third parties via free and/or interoperable formats and to set up communication channels with other organizations.

Clear documentation of processing bases, including consent, is mandatory to demonstrate compliance and ensure that consent is reflected in terms of data. However, transparency requirements also relate to the way in which these bases and consent items are presented to users, and there is evidence of discrepancies between how processing purposes are communicated and how the actual data processing occurs (Kurtz et al., 2020). Bergram et al. (2020) also analyze common methods for acquiring consent in digital settings, and both studies derive design

recommendations for enlightened user consent. Although this sub-capability emphasizes technological aspects, our tool analysis reveals that features related to data transfer are the least frequent.

Compliant processing demonstration (C2). This capability involves the ability to respond to inquiries from public authorities (art. 31) and denotes the ability to coordinate data protection activities with external data processors. It was derived from the principle of accountability (art. 24 § 1) (Bensoussan et al., 2018; Nicolaidou and Georgiades, 2017; Voigt and Von Dem Bussche, 2017).

EU-GDPR makes a distinction between data controllers and processors, and art. 28 orders the former to control compliance of the latter. This distinction is relevant to organizations when they outsource data processing to third-party companies—including the use of cloud services, as merely storing data is considered processing. This became apparent during the Allmed project (cloud CRM) and especially in the case of Leares, which exclusively relies on cloud services (e.g., CRM, content management, and websites) for the storage and processing of data.

Art. 31 specifies that organizations "shall cooperate, on request, with the supervisory authority in the performance of its tasks." This implies that organizations set up a contact person for authorities (usually the DPO) and are able to present relevant information/documentation as proof of compliance. Since such documentation should contain all relevant information regarding an organization's data protection practices, this capability is also about ensuring that said documentation considers the processing of data by third parties on behalf of the organization and is readily available for governmental review. The resulting sub-capabilities are:

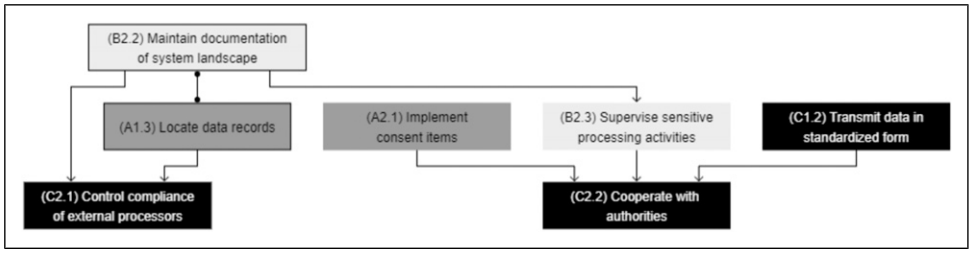

Figure 9. Capability relationships: Compliant processing demonstration (C2).

Table 10. Capability overview: Compliant processing demonstration (C2).

Sub-capability	Description	Specification	Implementation options and exemplary resources*	Compl. requirement (CR)
Control compliance of external processors (C2.1)	Ability to ensure that processing activities conducted by external processors comply with legal requirements	Only processors providing a sufficient guarantee of EU-GDPR compliance should be selected Documentation of processing activities Collaboration between organization and processors to guarantee the exercise of rights and proof of compliance Deletion or restitution of data at the end of the contract	Contract with processors with enhanced data protection terms (I) Vendor inventory (I) Enterprise architecture tools (T)	Art. 24 § 2 Art. 28 R. 58, 74, 78, 81-83, 101, 108, 111
Cooperate with authorities (C2.2)	Ability to collaborate with designated government bodies and communicate requested information	Records of processing activities Evidence of compliance and security measures Data breach notification	Contact person for authorities (H) Incident response processes (I) Documentation material (I)	Art. 17 Art. 31 Art. 33 Art. 39 § 1(d) R. 85, 87, 89, 94

*Technological – T / Human – H / Intangible – I.

- *Control compliance of external processors (C2.1):* ability to ensure that processing activities conducted by external processors comply with legal requirements.
- *Cooperate with authorities (C2.2):* ability to collaborate with designated government bodies and communicate requested information.

Similar to 4.5.1, these sub-capabilities may be seen as further operationalization of the principle of accountability, which is materialized through documentation and processes. When it comes to making sense of third-party data processing, enterprise architecture may also be used to document "external" processing systems (e.g., cloud storage). We have identified two software solutions that assist organizations in maintaining an inventory of all the vendors they use. In research, two studies have been published on the matter and focus on the issues of third-party data processing (Kurtz et al., 2018), as well as an investigation of third-party data dissemination in digital service ecosystems (Kurtz et al., 2019). The latter illustrates the challenges from both legal and technical perspectives in the seemingly straightforward use case of a weather app on a smartphone, which transmits data to the operating system provider, the app developer, and an underlying API provider.

Clear documentation of processing bases, including consent, is mandatory to demonstrate compliance. A variety of tools among all considered categories exhibit audit trail functionalities, which record and gather information about data processing and related events.

Building the capabilities

While the capability model comprises the relevant capabilities for achieving EU-GDPR compliance, the focus groups, case study, and expert interviews also highlighted different ways of using the capability model to support EU-GDPR initiatives in their different stages.

In the initial stage, the capability model aids exchanges and communication between legal and data management functions and establishes a common understanding of regulatory requirements. It extends data management professionals' knowledge of EU-GDPR compliance, which typically focuses narrowly on data objects and attributes—as confirmed by the consultant in the Shippy project: *"The capability model is very useful and goes beyond the 'obvious' aspects of the regulation. Many of [the capabilities] do not come to data managers' minds in the first place because the GDPR might be simplified to a perspective of whether I know which records represent a natural person and which don't."*

Beyond creating a basic understanding about the regulation, the capability model proved to be useful for evaluating an organization's current state of practice and distinguish areas of attention. Leares, like many other small and medium-sized companies, had compiled a lengthy to-do list compiled with the most visible and pressing compliance issues (e.g., adapting web forms, newsletters, and contracts) in order achieve what was considered a "minimum" level of compliance. These action items were presented as isolated items and focused mostly on technical issues, with no

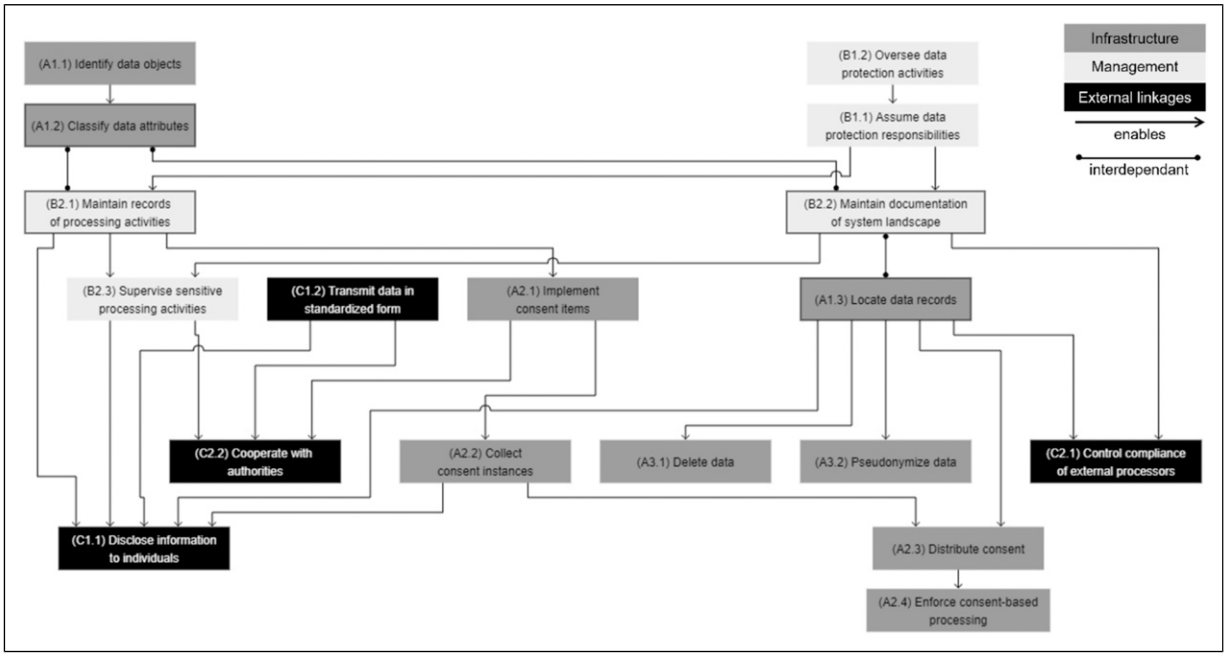

Figure 10. Capability network (see Appendix 4).

indication of why certain actions were necessary, or what compliance issue they were meant to fix. Using the capability model helped Leares in identifying compliance gaps as well as defining and prioritizing actions. Going through the model, they assigned each check-list activity to the related sub-capabilities and assessed to what extent they contributed to achieving compliance. When capabilities were partially covered by those activities, the model provided guidance to refine them. The capability model also helped identifying capabilities that Leares had not considered at all, such as defining the protected data scope.

In the focus groups and projects, most companies were overwhelmed when they saw the capabilities and realized that the gaps cannot easily be filled. In line with the RBV, they entail building capabilities as "complex patterns of coordination" between different types of resources (Grant, 1991), which also explains the difficulties with achieving timely compliance. In building the capabilities, understanding the dependencies is crucial for deciding on implementation priorities and defining a roadmap. The consultant at Shippy emphasized this point: *"What I really like about the model is [its] attempt to address the dependencies between capabilities. From a data management perspective, a typical challenge is: 'Now that I've identified a plethora of gaps and I've thought about what to do with which one, still, what is the sequence? With what do I need to start first? What are the "must-haves"'?"* Figure 10 depicts the relationships between the sub-capabilities as a network. It should be read from top to bottom, as arrows describe dependencies, where the source is a prerequisite to the target. The network shows the multipronged aspect of data protection for enterprises, meaning that achieving compliance requires a combination of three groups of capabilities—infrastructure, management, and external linkages capabilities—and cannot only be tackled from a data object–centric perspective or with a simple tool implementation.

In building the capabilities, organizations may employ a "bottom-up" approach (i.e., starting by tackling infrastructure capabilities) or a "top-down approach" (i.e., starting by addressing management capabilities). In the bottom-up approach, organizations would first perform an exploration of their technological resources at the physical level, for instance by scanning databases and data records (either manually or using automated tools) to identify and classify data objects that may contain personal data (A1.1 and A1.2). In the top-down approach, organizations would start by setting up responsibilities for data protection (B1.1 and B1.2) and building an understanding of the way personal data is processed at the conceptual level. Versuisse and Svizzance were two examples of top-down approaches, as they both emphasized establishing clear reporting lines, thus orchestrating data protection activities (B1). In the case of Svizzance, the company had achieved major progress on the documentation of processing activities and system landscape (B2) and was in the process of linking this documentation to data records (i.e., identifying data objects, classifying data attributes, and locating data records). However, it had not yet started activities related to consent processing (A2) and data removal (A3), as our respondents regarded having a clearly defined protected data scope as a prerequisite. A similar pattern was identified at Versuisse, which was more mature in defining the protected data scope and had just started venturing into consent processing and data removal capabilities at an enterprise-wide level. As insurance companies, Versuisse and Svizzance both operate in a highly regulated market. Such organizations traditionally emphasize control activities and maintain thorough documentation of their operations, which can explain the top-down approach that we have observed (i.e., starting from high-level documentation and investigating links and relationships with data objects). However, we argue that organizations that operate in markets with lower regulatory pressure or are, by their nature, data-driven could also adopt a bottom-up approach (i.e., starting by creating a list of data objects and classifying them to build or enhance their documentation of processing activities and system landscape). Leares is an example of the bottom-up approach, as such documentation did not exist and was built alongside the inventory of systems processing data in the protected data scope.

As depicted by Figure 10, whatever the approach, maintaining documentation of activities performed in either approach starts early in the capability-building process. Our analysis of capability relationships confirms that putting together documentation that reconciles physical and conceptual data layers (B2.1 and B2.2) is a prerequisite to making compliance activities efficient and plays a pivotal role in enterprises' ability to comply with data protection regulations. This is especially true for large organizations, where an informal understanding of data location (A1.3) or processing activities (B2.1) would inevitably result in compliance silos, which would directly contradict data protection rights and accountability requirements. These findings call back the essence of capabilities as "complex patterns of coordination" (Grant 1991) between technological, human, and intangible resources in the context of data protection. They also underline that achieving EU-GDPR compliance is an ongoing capability-building process.

Conclusion and outlook

Contributions

The EU-GDPR introduces a paradigm shift in data protection regulations, but the academic discourse on this topic is still nascent and lacks consolidation and theoretical integration. Building on the RBV, this paper argues that compliance with the EU-GDPR require companies to

mobilize technological, human, and intangible resources and build a dedicated set of enterprise-wide data management capabilities. Our main contribution is a comprehensive, theoretically and empirically grounded capability model for EU-GDPR, which comprises 7 capabilities and 18 sub-capabilities, grouped in infrastructure and management capabilities, as well as external linkages. By translating compliance requirements into capabilities, we advance research at the intersection between legal and IS domains with two main contributions: First, we analyze EU-GDPR, which represents the latest generation of data protection regulations, by using concepts from the RBV, as well as regulatory compliance management literature (El Kharbili, 2012). We introduce capabilities as means to systematically interpret and translate data protection compliance requirements and connect them to implementation options and the required resources. In that sense, we link compliance rules and practice in the spirit of the sense-making dimension of IT-based regulation (de Vaujany et al., 2018). Furthermore, we address a gap in regulatory compliance literature, as our findings derive corrective solutions, that is, providing guidance to reach strategic compliance objectives (Cleven and Winter, 2009) from legal analysis, as opposed to preventive or detective solutions (Abdullah et al., 2009). Second, by linking the regulation to the resource-based view, we propose an enterprise-wide perspective of the *what* of EU-GDPR implementation rather than the *how*. Thus, the capability model complements the fragmented body of research on EU-GDPR and extends the scope beyond the isolated investigation of specific implementation options by classifying and integrating these focused research efforts into an enterprise-wide perspective. It also informs the materialization relationship between rules and IT artifacts (de Vaujany et al., 2018) by elaborating on different ways in which rules can be expressed as part of IT design (via dedicated infrastructure capabilities, among others, and by providing a framework to classify IT-based implementation options). Finally, our study enriches the privacy research domain in information systems by analyzing the oft-neglected legal component of information privacy, thereby heeding the call for privacy research to be conducted at the organizational rather than the individual level (Bélanger and Crossler, 2011; Smith et al., 2011).

Implications

As a mature research stream, the RBV helps to explain the difficulties faced by companies with achieving compliance, even several years after EU-GDPR entered into force. The capability model, taken together with practical insights and the analysis of available implementation options, illustrates that no single tool or approach can fulfill all of the regulation's requirements. It highlights that data protection compliance calls for enterprise-wide approaches, and that achieving EU-GDPR compliance is not a one-time effort but an ongoing capability-building process that relies on a combination of technological, human, and intangible resources. The three groups of capabilities—infrastructure, management, and external linkages capabilities—show that EU-GDPR compliance requires a wide range of capability types, including capabilities that are deployed inside the enterprise ("inside-out" capabilities according to Wade and Hulland's (2004) typology) as well are externally oriented capabilities ("outside-in" capabilities, *ibid.*) that create relationships with authorities and data subjects. While prior research has suggested specific solutions to tackle selected aspects of the regulation, the capability model acts as a framework to determine the scope of these solutions, assess gaps and priorities, and illustrate their interplay. For future research, the capability model provides a framework that allows to theorize about the capabilities required for EU-GDPR-compliant data management, position and compare suggestions for EU-GDPR-compliant solutions in the larger context, and generalize beyond the EU-GDPR.

In practice, the capability model supports companies to develop a systematic approach that would enable them to comply with the EU-GDPR and monitor progress instead of "fire-fighting." According to the experts, it offers a comprehensive perspective of the prerequisites for achieving compliance and draws attention to aspects "*beyond the obvious requirements, such as consent*," which are often overlooked by IT and data professionals. The projects carried out as part of our research process demonstrate that companies can use the capability model in different ways: first, as a basis for assessing their current data management capabilities in light of the regulation by identifying the required capabilities and prioritizing them; second, by analyzing software features that help fulfill their capabilities and map them to existing market offerings, thus further informing EU-GDPR implementation initiatives; third, by monitoring progress toward compliance and, thus, supporting the development of capabilities.

Limitations and avenues for future research

While this study does have limitations, it also offers interesting opportunities for future research. First, we acknowledge that the capability model is specific to the EU-GDPR. However, we argue that the identified capabilities are relevant beyond this regulation and its regional scope. As already mentioned, many countries have revised their data protection regulations in recent years or are in the process of doing so. While every country defines specific rules, EU-GDPR has set a global standard, and other regulations are building on similar concepts, as evident in the examples of California, India, and Japan. Furthermore,

companies with global operations have to comply with an increasing number of country- and industry-specific data protection regulations. The approach suggested in this paper may serve as a basis for analyzing commonalities and differences between regulations, as well as identifying a "common core." As EU-GDPR has set global standards as a very strict regulation, we can also assume that the identified capabilities are likely to foster compliance with other regulations.

Second, our findings may be biased by the companies that contributed to the design of the capability model. Interestingly, we did not observe industry-specific differences in their approach to achieve compliance. Even B2B companies (machinery, automotive) were highly impacted by the regulation—for instance, because they interact with their (end) customers and partners through of a growing number of websites and digital channels. Nevertheless, we acknowledge that industry-specific compliance requirements and approaches deserve more research.

Another limitation is that we concentrate our research efforts on the capability model as a means to achieve compliance goals but do not substantiate the capabilities' impact on firm performance. Future research should study the links between capabilities and control objectives derived from regulatory requirements, as well as measure their impact on the firm performance. In fact, non-compliance bears risk of high fines and reputation loss, which negatively impacts firm performance. At the same time, the strict rules imposed by the EU-GDPR can harm value-adding, data-driven activities in the enterprise. Interestingly, we also found evidence that certain capabilities (e.g., transparency on data flows, storage, and usage) are not specific to EU-GDPR and may also serve other purposes in organizations as a way to outweigh potential conflicting interest that some researchers have identified (Engels, 2016; Grundstrom et al., 2020; Jakobi et al., 2020; Lindgren, 2020; Martin and Matt, 2018; Wohlfarth, 2019). Therefore, we see the dichotomy between compliance and business value, and the questioning thereof, as a promising avenue for future research.

Acknowledgments

The authors would like to thank the CC CDQ partner companies for their financial support and their active contributions to this research.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Competence Center Corporate Data Quality (CC CDQ).

ORCID iDs

Clément Labadie https://orcid.org/0000-0002-3545-3638
Christine Legner https://orcid.org/0000-0001-8891-3813

Supplemental Material

Supplemental material for this article is available online.

Notes

1. The first version of the capability model was published in a conference paper: *Labadie, C., Legner, C., 2019. Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR, in: Proceedings of the 14th International Conference on Wirtschaftsinformatik (WI). Siegen, Germany, (*https://aisel.aisnet.org/wi2019/track11/papers/3/*)*.
2. Regulation (EU) 2016/679. All recitals (R.) and articles (art.) refer to the EU-GDPR, unless otherwise specified.
3. Over 10 industries are represented in the research program, including pharmaceuticals, retail, engineering, telecommunications, fast-moving consumer goods, software, automotive, and chemistry.
4. All company names have been anonymized.
5. For displaying the dependencies between sub-capabilities, we use an outward arrow to depict an enablement relationship, an inward arrow a dependency relationship, and a point-to-point arrow an interdependency relationship. The color represents the capability group: Infrastructure capabilities are colored in dark gray, management capabilities in light gray, and external linkages capabilities in black. This applies to all subsequent capability relationships figures.

References

Abdullah NS, Indulska M and Shazia S (2009) A study of compliance management in information systems research. In: Proceedings of the 17th European conference on information systems (ECIS), Verona, Italy, 8 June, p. 5.

Addis C and Kutar M (2020) General data protection regulation (GDPR), artificial intelligence (AI) and UK organisations: a year of implementation of GDPR. In: Proceedings of the 25th UK academy for information systems annual conference (UKAIS). Oxford, United Kingdom, 31 April https://aisel.aisnet.org/ukais2020/24

Addis M and Kutar M (2018) The general data protection regulation (GDPR), emerging technologies and UK organisations: awareness, implementation and readiness. In: Proceedings of the 23rd UK academy for information systems annual conference (UKAIS). Oxford, United Kingdom, 20 March, p. 29. https://aisel.aisnet.org/ukais2018/29

Alboaie L (2017) Towards a smart society through personal assistants employing executable choreographies. In: Proceedings of the 26th international conference on information

systems development (ISD), Larnaca, Cyprus, 6 September, p. 5.

Armingaud C-E and Ligot A (2019) Le Consentement: Le Faux-Ami Des Bases Légales. *Revue Lamy Droit de l'Immatériel* 160: 44–46.

Baiyere A and Salmela H (2014) Towards a unified view of information system (IS) capability. In: Proceedings of the 18th Pacific Asia conference on information systems (PACIS), Chengdu, China, 24 June, p. 329.

Barney J (1991) Firm resources and sustained competitive advantage. *Journal of Management* 17(1): 99–120.

Barney JB (2001) Resource-based theories of competitive advantage: a ten-year retrospective on the resource-based view. *Journal of Management* 27(6): 643–650. https://doi.org/10.1177/014920630102700602

Bélanger F and Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly* 35(4): 1017–1042.

Bensoussan A, Avignon C, Bensoussan-Brulé V, et al. (2018) *Règlement Européen Sur La Protection Des Données: Textes, Commentaires et Orientations Pratiques*. 2nd ed. Brussels: Bruylant.

Bergram K, Bezençon V, Maingot P, et al. (2020) Digital nudges for privacy awareness: from consent to informed consent? In: Proceedings of the 28th European conference on information systems (ECIS), Marrakesh, Morocco, 15 June, p. 64. https://aisel.aisnet.org/ecis2020_rp/64

Bharadwaj A (2000) A resource-based perspective on information technology capability and firm performance: an empirical investigation. *MIS Quarterly* 24(1): 169–196.

Bharadwaj A, Sambamurthy V and Zmud R (1999) IT capabilities: theoretical perspectives and empirical operationalization. In: Proceedings of the 20th international conference on information systems, Charlotte, NC, USA, 13 December, p. 35.

Buchwald A, Urbach N and Ahlemann F (2014) Business value through controlled IT: toward an integrated model of IT governance success and its impact. *Journal of Information Technology* 29(2): 128–147. https://doi.org/10.1057/jit.2014.3

Burmeister F, Drews P and Schirmer I (2019) A privacy-driven enterprise architecture meta-model for supporting compliance with the general data protection regulation. In: Proceedings of the 52nd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 8 January. https://doi.org/10.24251/HICSS.2019.729

Burmeister F, Huth D, Drews P, et al. (2020) Enhancing information governance with enterprise architecture management: design principles derived from benefits and barriers in the GDPR implementation. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.688

Butler T and O'Brien L (2019) Understanding RegTech for digital regulatory compliance. In: Lynn T, Mooney JG, Rosati P, et al (eds) *Disrupting finance: FinTech and strategy in the 21st century, palgrave studies in digital business & enabling technologies*. Cham: Springer International Publishing, 85–102. https://doi.org/10.1007/978-3-030-02330-0_6

California State Senate (2018) *California Consumer Privacy Act*.

Capgemini Research Institute (2019) Championing data protection and privacy - a source of competitive advantage in the digital century. Consultancy Report. Consultancy Report, September. https://www.capgemini.com/wp-content/uploads/2019/09/Report_Championing-Data-Protection-and-Privacy.pdf

Castets-Renard C (2019) Accountability of algorithms in the GDPR and beyond: a European legal framework on automated decision-making. *Fordham Intellectual Property, Media and Entertainment Law Journal* 30(1): 91.

Chatellier R, Delcroix G and Hary E (2019) "La Forme Des Choix - Données Personnelles, Design et Frictions Désirables," Research Report No. 06, Cahiers IP Innovation & Prospective, Research Report, Commission Nationale de l'Informatique et des Libertés.

Cheffert J. M. 2018. Respect de La Vie Privée : Quand Les Approches Économiques et Juridiques Se Rejoignent. In *Law, Norms and Frefoms in Cyberspace - Droit, Normes et Libertés Dans Le Cybermonde - Liber Amicorum Yves Poullet, Collection*, edited by Du CRIDS, E Degrave, C de Terwangne, S Dusollier and R Queck, 505-524. Brussels: Larcier.

Cleven A and Winter R (2009) Regulatory compliance in information systems research - literature analysis and research agenda. In: *Enterprise, Business Process and Information Systems Modeling, Lecture Notes in Business Information Processing*. Berlin, Heidelberg: Springer-Verlag, 174–186.

Commission Nationale de l'Informatique et des Libertés (n.d.). Lignes directrices et recommandations de La CNIL. (https://www.cnil.fr/fr/decisions/lignes-directrices-recommandations-CNIL (Accessed May 26, 2021).

Dansac Le Clerc M and Mannent P (2020) "GDPR Survey - Benefits Beyond Compliance," Consultancy Report, Consultancy Report, Baker McKenzie & BearingPoint, April. https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/gdpr_survey.pdf?la=en

De Hert P and Malgieri G (2018) Making the most of new laws: reconciling big data innovation and personal data protection within and beyond the GDPR. In: Degrave E, de Terwangne C, Dusollier S, et al. (eds) *Law, Norms and Frefoms in Cyberspace - Droit, Normes et Libertés Dans Le Cybermonde - Liber Amicorum Yves Poullet, Collection Du CRIDS*. Brussels: Larcier, 525–554.

De Hert P and Papakonstantinou V (2012) The proposed data protection regulation replacing directive 95/46/EC: a sound system for the protection of individuals. *Computer Law & Security Review* 28(2): 130–142. https://doi.org/10.1016/j.clsr.2012.01.011

De Hert P and Papakonstantinou V (2016) The new general data protection regulation: still a sound system for the protection of

individuals? *Computer Law & Security Review* 32(2): 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

de Vaujany FX, Fomin VV, Haefliger S and Lyytinen K (2018) Rules, practices, and information technology: A trifecta of organizational regulation. *Information Systems Research* 29(3): 755–773. https://doi.org/10.1287/isre.2017.0771

Debet A (2018) Les Nouveaux instruments de Conformité. In: *Le RGPD, Grand Angle*. Paris: Dalloz, 67–72.

Debet A, Massot J and Métallinos N (2015) *Informatique et Libertés: La Protection Des Données à Caractère Personnel En Droit Français et Européen, Les Intégrales*. Issy-les-Moulineaux: Lextenso.

Diamantopoulou V and Mouratidis H (2018) Evaluating a reference architecture for privacy level agreement's management. In: Proceedings of the 12th Mediterranean conference on information systems (MCIS), Corfu, Greece, 28 September, p. 28. https://aisel.aisnet.org/mcis2018/28

Docquir B (2018) *Droit Du Numérique, Répertoire Pratique Du Droit Belge*, (R. Andersen, J. du Jardin, P. A. Foriers, and L. Simont, eds.), Brussels: Larcier.

El Kharbili M (2012) Business process regulatory compliance management solution frameworks: a comparative evaluation. In: Proceedings of the 8th Asia-Pacific conference on conceptual modelling (APCCM), Melbourne, Australia, 30 January 2012, 130, pp. 23–32. http://dl.acm.org/citation.cfm?id=2523782.2523786

Engels B (2016) Data portability and online platforms the effects on competition. In: Proceedings of the 29th bled EConference (BLED), Bled, Slovenia, 19 June, p. 39.

European Commission (2020) *A European Strategy for Data," Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committe of the Regions No. COM(2020) 66 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committe of the Regions*. Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Data Protection Board (2017) *"Guidelines on Data Protection Officers (WP243 Rev.01)," Regulatory Guidelines, Regulatory Guidelines*. European Union, May 4.

European Data Protection Board (2018a) *"Guidelines on Transparency under Regulation 2016/679 (WP260 Rev.01)," Regulatory Guidelines, Regulatory Guidelines*. European Union, November 4.

European Data Protection Board (2018b) *"Guidelines On Consent Under Regulation 2016/679 (WP259, Rev.01)," Regulatory Guidelines, Regulatory Guidelines*. European Union, October 4.

European Data Protection Supervisor (2018) "Avis Préliminaire Sur Le Respect de La Vue Privée Dès La Conception," Government Report No. Avis 5/2018, Government Report, European Union.

European Data Protection Supervisor (2019) *Annual Report 2019*. European Union: Government Report, Government Report.

European Union Agency for Fundamental Rights (2018) European Court of Human Rights, Council of Europe, and European Data Protection SupervisorManuel de Droit Européen En Matière de Protection Des Données. 2018th ed. Luxemburg: Office des Publications de l'Union Européenne.

Faber B, Michelet GC, Weidmann N, et al. (2020) BPDIMS: a blockchain-based personal data and identity management system. In: Proceedings of the 52nd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 8 January. https://doi.org/10.24251/HICSS.2019.821

Farshid S, Reitz A and Roßbach P (2019) Design of a forgetting blockchain: a possible way to accomplish GDPR compatibility. In: Proceedings of the 52nd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 8 January. https://doi.org/10.24251/HICSS.2019.850

Fellous-Sigrist M (2018) Consent in the digital context: the example of oral history interviews in the United Kingdom. In: *La Diffusion Numérique Des Données En SHS - Guide de Bonnes Pratiques Éthiques et Juridiques*. Aix-en-Provence: Presses universitaires de Provence. https://hal-amu.archives-ouvertes.fr/hal-02058184

Fox G, Tonge C, Lynn T, et al. (2018) Communicating compliance: developing a GDPR privacy label. In: Proceedings of the 24th Americas conference on information systems (AMCIS), New Orleans, Louisiana, USA, 16 August, p. 30.

Francis M, Covert Q, Steinhagen D, et al. (2020) An inventory of international privacy principles: a 14 country analysis. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.534

Govindarajan V, Srivastava A and Enache L (2019) How India Plans to Protect Consumer Data. *Harvard Business Review*. https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data

Grant RM (1991) The resource-based theory of competitive advantage: implications for strategy formulation. *California Management Review* 33(3): 114.

Groos D and Veen E-Bv (2020) Anonymised data and the rule of law. In: *European Data Protection Law Review (6:4)*: Lexxion Publisher, 498–508. https://doi.org/10.21552/edpl/2020/4/6

Grundstrom C, Väyrynen K, Iivari N, et al. (2020) Making sense of the general data protection regulation—four categories of personal data access challenges. In: Proceedings of the 52nd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 11 Jaunary https://doi.org/10.24251/HICSS.2019.605

Guggenmos F, Lockl J, Rieger A, et al. (2020) How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the german asylum procedure. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui,

Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.492

Heier H, Borgman HP and Maistry Mg (2007) Examining the relationship between IT governance software and business value of IT: evidence from four case studies. In: Proceedings of the 40th Hawaii international conference on system sciences (HICSS), Waikoloa Village, Hawaii, USA, 3 January, p. 234. https://doi.org/10.1109/HICSS.2007.216

Helfat CE and Peteraf MA (2003) The dynamic resource-based view: capability lifecycles. *Strategic Management Journal* 24(10): 997–1010.

Hevner AR, March ST, Park J, et al. (2004) Design science in information systems research. *MIS Quarterly* 28(1): 75–105.

Hoeren T and Kolany-Raiser B (2018) *The Importance of Data Quality for Big Data," in Law, Norms and Frefoms in Cyberspace - Droit, Normes et Libertés Dans Le Cybermonde - Liber Amicorum Yves Poullet, Collection Du CRIDS*, E. Degrave, C. de Terwangne, S. Dusollier, and R. Queck (eds.), Brussels: Larcier, 619–636.

Houta S, Meschede C, Beeres K, et al. (2020) User-centered design and evaluation of standard-based health technologies for epilepsy care. In: Proceedings of the 28th European conference on information systems (ECIS), Marrakesh, Morocco, 15 June, p. 16. https://aisel.aisnet.org/ecis2020_rp/16.

Huth D, Both A, Ahmad J, et al. (2020) Process and tool support for integration of privacy aspects in agile software engineering. In: Proceedings of the 26th Americas conference on information systems (AMCIS), Salt Lake City, Utah, USA, 15 August, p. 6. https://aisel.aisnet.org/amcis2020/systems_analysis_design/systems_analysis_design/6

Huth D, Burmeister F, Matthes F, et al. (2020) Empirical results on the collaboration between enterprise architecture and data protection management during the implementation of the GDPR. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.715

Huth D and Matthes F (2019) 'Appropriate technical and organizational measures': identifying privacy engineering approaches to meet GDPR requirements. In: Proceedings of the 25th Americas Conference on Information Systems (AMCIS), Cancún, Mexico, 15 August, p. 4. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/5

Iannopollo E, Balaouras S and Harrison P (2017) *"The Five Milestones to GDPR Success," Executive Brief, Executive Brief*. Forrester Research, April 25.

Iannopollo E, Balaouras S, Pikulik E, et al. (2018) *"The State of GDPR Readiness," Executive Brief, Executive Brief*. Forrester Research, January 31.

Information Commissioner's Office (2017) *Consultation: GDPR Consent Guidance*. Government Report, Government Report.

Jakobi T, von Grafenstein M, Legner C, et al. (2020) The role of IS in the conflicting interests regarding GDPR. *Business & Information Systems Engineering* 62(3): 261–272. https://doi.org/10.1007/s12599-020-00633-4

Japan Personal Information Protection Commission (2020) *Amended Act on the Protection of Personal Information*. https://www.ppc.go.jp/files/pdf/APPI_english.pdf

Karjoth G and Langheinrich M (2019) *"Technische Gestaltung von Informed Consent,"* Digma: Zeitschrift Für Datenrecht Und Informationssicherheit, 72–79.

Karyda M and Mitrou L (2016) Data breach notification: issues and challenges for security management. Proceedings of the 10th Mediterranean conference on information systems(MCIS), Paphos, Cyprus, 4 September, p. 60.

Kurtz C, Semmann M and Böhmann T (2018) Privacy by design to comply with GDPR: a review on third-party data processors. In: Proceedings of the 24th Americas conference on information systems, New Orleans, LA, USA, 16 August. https://aisel.aisnet.org/amcis2018/Security/Presentations/36

Kurtz C, Wittner F, Semmann M, et al. (2019) The unlikely siblings in the GDPR family: a techno-legal analysis of major platforms in the diffusion of personal data in service ecosystems. In: Proceedings of the 52nd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 8 January. https://doi.org/10.24251/HICSS.2019.607

Kurtz C, Wittner F, Vogel P, et al. (2020) Design goals for consent at scale in digital service ecosystems. In: Proceedings of the 28th European conference on information systems (ECIS), Marrakesh, Morocco, 15 June, p. 69. https://aisel.aisnet.org/ecis2020_rp/69

Labadie C and Legner C (2019) Understanding data protection regulations from a data management perspective: a capability-based approach to EU-GDPR. In: Proceedings of the 14th international conference on wirtschaftsinformatik (WI), Siegen, Germany, 23 February. https://aisel.aisnet.org/wi2019/track11/papers/3/

Labadie C and Legner C (2020) Personal data management inside and out - Integrating data protection regulations in the data life cycle. *Enterprise Modelling and Information Systems Architectures* 15(9). https://doi.org/10.18417/emisa.15.9

Lazaro C and Le Métayer D (2015) Control over personal data: true remedy or fairy tale? SCRIPT-Ed (12:1), p. 32.

Legner C, Pentek T and Otto B (2020) Accumulating design knowledge with reference models: insights from 12 years of research on data management. *Journal of the Association for Information Systems* 21(3).

Lindgren P (2020) The impact on multi business model innovation related to GDPR regulation. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.537

Martin N and Matt C (2018) Unblackboxing the effects of privacy regulation on startup innovation. In: Proceedings of the 39th international conference on information systems (ICIS), San Francisco, California, USA, 13 December, p. 11. https://aisel.aisnet.org/icis2018/security/Presentations/11

Martinez J, Ruiz A, Puelles J, et al. (2019) Smart grid challenges through the lens of the european general data protection

regulation. In: Proceedings of the 28th international conference on information systems development(ISD), Toulon, France, 28 August, p. 4. https://aisel.aisnet.org/isd2014/proceedings2019/Society/4

Mathiassen L (2002) Collaborative Practice Research. *Information Technology & People* 15(4): 321–345. https://doi.org/10.1108/09593840210453115

Maunula G (2020) Advancing technological state-of-the-art for GDPR compliance: considering technology solutions for data protection issues in the sharing economy. *Journal of the Midwest Association for Information Systems (JMWAIS)* 2020(2): 4. https://doi.org/10.17705/3jmwa.000060

Meier P (2011) *Protection Des Données: Fondements, Principes Généraux et Droit Privé, Précis de droit Stämpfli*. Bern: Stämpfli.

Mejtoft T, Hellman D and Söderström U (2019) Reclaiming control over personal data with blockchain technology: an exploratory study. In: Proceedings of the 32nd bled EConference (BLED), Bled, Slovenia, 16 June, pp. 411–425. http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-160870.

Métille S and Raedler D (2017) Swiss data protection act reform set in motion. *Data Protection Leader* 14(2): 14–16.

Mitrou L (2017) The general data protection regulation: a law for the digital age? In: Jougleux P, Markou C and Prastitou T (eds) *EU Internet Law: Regulation and Enforcement, T.-E. Synodinou*. Cham: Springer International Publishing, pp. 19–57. https://doi.org/10.1007/978-3-319-64955-9_2

Naftalski F (2018) *Feuille de Route : Les Incontournables, in Le RGPD, Grand Angle*. Paris: Dalloz, pp. 253–259.

Nicolaidou IL and Georgiades C (2017) The GDPR: new horizons. In: Synodinou T-E, Jougleux P, Markou C, et al. (eds) *EU Internet Law: Regulation and Enforcement*. Cham: Springer International Publishing, 3–18. https://doi.org/10.1007/978-3-319-64955-9_1

Österle H and Otto B (2010) Consortium research: a method for researcher-practitioner collaboration in design-oriented IS research. *Business & Information Systems Engineering* 2(5): 283–293. https://doi.org/10.1007/s12599-010-0119-3

Pankowska M (2018) Privacy awareness in the GDPR implementation circumstances. In: Proceedings of the 27th international conference on information systems development (ISD), Lund, Sweden, 22 August, p. 5. https://aisel.aisnet.org/isd2014/proceedings2018/Transforming/5

Paul C, Scheibe K and Nilakanta S (2020) Privacy concerns regarding wearable IoT devices: how it is influenced by GDPR? Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.536

Peffers K, Tuunanen T, Rothenberger MA, et al. (2007) A design science research methodology for information systems research. *Journal of Management Information Systems* 24(3): 45–77. https://doi.org/10.2753/MIS0742-1222240302

Petkov P and Helfert M (2017) Identifying emerging challenges for ICT Industry in Ireland: multiple case study analysis of data privacy breaches. In: Proceedings of the 23rd Americas conference on information systems (AMCIS), Boston, Massachussetts, USA, 10 August, p. 40.

Prat N, Comyn-Wattiau I and Akoka J (2015) A taxonomy of evaluation methods for information systems artifacts. *Journal of Management Information Systems* 32(3): 229–267. https://doi.org/10.1080/07421222.2015.1099390

Presthus W and Sørum H (2019) Consumer perspectives on information privacy following the implementation of the GDPR. *International Journal of Information Systems and Project Management* 7(3): 19–34.

Proferes N and Walker S (2020) Researcher views and practices around informing, getting consent, and sharing research outputs with social media users when using their public data. In: Proceedings of the 53rd Hawaii international conference on system sciences (HICSS), Maui, Hawaii, USA, 7 January. https://doi.org/10.24251/HICSS.2020.290

Puyraimond J-F (2019) L'intérêt Légitime Du Responsable Du Traitement Dans Le RGPD: In Cauda Venenum? *Droit de La Consommation* 1(122): 39–77.

Rallet A, Rochelandet F and Zolynski C (2015) De la Privacy by Design à la Privacy by Using. In: *Reseaux (189:1)*. La Découverte, 15–46.

Rieger A, Guggenmos F, Lockl J, et al. (2019) Building a blockchain application that complies with the EU general data protection regulation. *MIS Quarterly Executive* 18(4): 263–279.

Ritschel A, Hochstein A, Josi M, et al. (2005) SOX-IT-compliance bei novartis. *HMD - Praxis der Wirtschaftsinformatik* 43(250): 68–77.

Rösch D, Schuster T, Waidelich L, et al. (2019) Privacy control patterns for compliant application of GDPR. In: Proceedings of the 25th Americas conference on information systems (AMCIS), Cancún, Mexico, 15 August. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/27

Rubio M (2019) *"To Impose Privacy Requirements on Providers of Internet Services Similar to the Requirements Imposed on Federal Agencies under the Privacy Act of 1974," No. S.142, Congress of the United States, January 16*.

Russell KD, O'Raghallaigh P, O'Reilly P, et al. (2018) Digital privacy GDPR: a proposed digital transformation framework. In: Proceedings of the 24th Americas conference on information systems (AMCIS), New Orleans, Louisiana, USA, 16 August, p. 36.

Sadiq S, Governatori G and Namiri K (2007) Modeling control objectives for business process compliance. In: Proceedings of the 5th International conference on business process management (BPM), Brisbane, Australia, 24 September, pp. 149–164.

Smith HJ, Dinev T and Xu H (2011) Information privacy research: an interdisciplinary review. *MIS Quarterly* 35(4): 989–1016.

Solove DJ (2013) Introduction: privacy self-management and the consent dilemma. *Harvard Law Review* 126(7): 1880–1903.

Staiger DN (2017) *Data protection compliance in the cloud," doctoral thesis*. Doctoral thesis, University of Zürich, Zürich, Switzerland.

Swiss Confederation (2020) *New Federal Act on Data Protection (nFADP)*, p. 92. https://fedlex.data.admin.ch/eli/fga/2020/1998

Synodinou T, Jougleux P, Markou C, et al. (eds), (2017) *EU Internet Law: Regulaton and Enforcement*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69583-5

Synodinou T, Jougleux P, Markou C, et al. (eds), (2021) *EU Internet Law in the Digital Single Market*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69583-5

Synodinou T-E, Jougleux P, Markou C, et al. (eds), (2020) *EU Internet Law in the Digital Era*. Cham: Springer International Publishing.

Tanaka H and Kitayama N (2020) Japan enacts amendments to the act on the protection of personal information. *International Association of Privacy Professionals*. https://iapp.org/news/a/japan-enacts-the-act-on-the-protection-of-personal-information/ (accessed 13 September 2021).

Thélisson E (2020) *Le Règlement Général Sur La Protection Des Données et Son Impact En Suisse," Doctoral thesis, Doctoral thesis*. Lausanne, Switzerland: University of Fribourg.

Tona O, Someh IA, Mohajeri K, et al. (2018) Towards ethical big data artifacts: a conceptual design. In: Proceedings of the 51st Hawaii international conference on system sciences (HICSS), Waikoloa Village, Hawaii, USA, 3 January. https://doi.org/10.24251/HICSS.2018.571

Veiga AD, Vorster R, Li F, et al. (2018) A comparison of compliance with data privacy requirements in two countries. In: Proceedings of the 26th European conference on information systems (ECIS), Portsmouth, United Kingdom, 23 June, p. 86. https://researchportal.port.ac.uk/portal/en/publications/a-comparison-of-compliance-with-data-privacy-requirements-in-two-countries(4d4793b4-5c62-475b-b9b4-801e93639944)/export.html.

Vemou K and Karyda M (2018) An evaluation framework for privacy impact assessment methods. In: Proceedings of the 12th Mediterranean conference on information systems (MCIS), Corfu, Greece, 28 September, p. 4. https://aisel.aisnet.org/mcis2018/5

Voigt P and Von Dem Bussche A (2017) *The EU general data protection regulation (GDPR): a practical guide*. Cham: Springer International Publishing.

Vom Brocke J and Buddendick C (2006) Reusable conceptual models–requirements based on the design science research paradigm. In: Proceedings of the 1st international conference on design science research in information systems and technology (DESRIST), Claremont, California, USA, 24 February 2006, pp. 576–604.

von der Leyen U (2020) *Statement by the President at 'Internet, a New Human Right'*. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_1999

Wade M and Hulland J (2004) The resource-based view and information systems research: review, extension, and suggestions for future research. *MIS Quarterly* 28(1): 107–142. https://doi.org/10.2307/25148626

Watson H and Nations C (2019) Addressing the growing need for algorithmic transparency. *Communications of the Association for Information Systems* 45(1): 488–510. https://doi.org/10.17705/1CAIS.04526

Wiese Schartum D (2018) Intelligible and effective data protection legislation. In: Degrave E, de Terwangne C, Dusollier S, et al. (eds) *Law, Norms and Frefoms in Cyberspace - Droit, Normes et Libertés Dans Le Cybermonde - Liber Amicorum Yves Poullet, Collection Du CRIDS*. Brussels: Larcier, 765–782.

Wohlfarth M (2019) Data portability on the internet. *Business & Information Systems Engineering* 61(5): 551–574. https://doi.org/10.1007/s12599-019-00580-9

Zanfir G (2014) Forgetting About consent. why the focus should be on 'suitable safeguards' in data protection law. In: Gutwirth S, Leenes R and De Hert P (eds) *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*. Dordrecht: Springer Netherlands, 237–257. https://doi.org/10.1007/978-94-007-7540-4_12

Zhang J, Hassandoust F and Williams J (2020) Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems* 12(1): 4. https://doi.org/10.17705/1pais.12104

Zhang M, Sarker S and Sarker S (2013) Drivers and export performance impacts of IT capability in 'born-global' firms: a cross-national study. *Information Systems Journal* 23(5): 419–443. https://doi.org/10.1111/j.1365-2575.2012.00404.x

Author biographies

Clément Labadie holds a PhD in Information Systems from the Faculty of Business and Economics (HEC), University of Lausanne Switzerland. His research focuses on the interplay between enterprise data management and the related compliance and legal frameworks.

Christine Legner is a professor of information systems at the Faculty of Business and Economics (HEC), University of Lausanne, Switzerland. She also serves as the academic director of the Competence Center Corporate Data Quality (CC CDQ), an industry-funded research consortium and expert community in the data management field. Her research interests relate to data management and data quality, business information systems, strategic IT planning, and enterprise architecture.