Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR

Clément Labadie[1], Christine Legner[1]

[1] Faculty of Business and Economics (HEC), University of Lausanne, Switzerland
{clement.labadie, christine.legner}@unil.ch

Abstract. The European General Data Protection Regulation (EU-GDPR) has entered into force in May 2018. Its emphasis on individual control and organizational accountability constitutes a new paradigm that requires changes in the way organizations manage personal data. However, organizations face difficulties when implementing EU-GDPR due to a lack of common ground between legal and data management domains. Anchored in the resource-based view theory (RBV), this paper argues that the regulation requires companies to build a dedicated data management capability. It presents a capability model that was developed in an iterative design science process, integrating both interpretation of legal texts and practical insights from focus groups with more than 30 experts and from 3 EU-GDPR projects. The paper advances the regulatory compliance management literature by translating legal data protection concepts for the IS community. It also contributes to practice by enabling organization to set-up systematic approaches towards EU-GDPR compliance.

Keywords: EU-GDPR, Data Protection, Regulations, Compliance, Capabilities.

1 Introduction

In 2017, The Economist published an article entitled "The world's most valuable resource is no longer oil, but data" [1], mirroring the transformation of our modern economies, in which massive data collection and analysis have become a key competitive advantage. This transformation had led the European Union (EU) to start a major reform of its data protection framework, which resulted in the adoption of the General Data Protection Regulation (EU-GDPR) in 2016, and its enforcement in May 2018. The EU-GDPR constitutes a paradigm shift in data protection, towards greater choice and sovereignty for individuals, and more accountability for organizations [2]. For organizations, it comes with the burden of proof related to whether, how and how well they protect personal data and increased fines for noncompliance. This requires them to fundamentally rethink the way they store and process personal data on an

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

enterprise-wide level. Despite the past deadline, most companies have not yet reached full EU-GDPR compliance. A study conducted in April 2018 among more than 1000 European and US companies reported that 40% of respondent organizations would not comply on May 25th, 2018. And even if companies have started to address GDPR, only 23% of US-based companies and 31% of EU-based companies stated that they were confident with their ability to comply [3].

The difficulties in implementing EU-GDPR highlight the general lack of common ground between legal and IS in both research and practice. From the research side, legal aspects of information privacy were not among the "topic areas closer to the interests of most IS researchers" [4], and the few IS studies on EU-GDPR have a very restricted scope. Similarly, in most companies, data protection topics have traditionally been addressed by legal departments by adapting contracts and general conditions, but without directly influencing data management practices. However, the new regulation does not allow for such a restricted approach, and companies see data processing related issues as the most challenging topics in EU-GDPR. In fact, preparing for data breach notification, operationalizing data portability, operationalizing the right to be forgotten and conducting data inventory/mapping were cited as "most difficult GDPR obligations to comply with" [3]. Furthermore, our interactions with practitioners indicate that the regulation is very generic, and that there is a need to translate it into data management concepts and practices. This "translation" would help analyze compliance requirements and options, before deciding on concrete (technical) implementations.

Anchored in the resource-based view theory (RBV), this paper argues for utilizing capabilities as an interface between abstract compliance requirements and their concretization. It aims at addressing the following research question: what data management capabilities need to be built in order to address EU-GDPR's requirements? Following a design science research approach, we propose a capability model for EU-GDPR that integrates both interpretation of legal texts and practical insights from focus groups with experts from 22 companies as well as 3 EU-GDPR related projects. The resulting capability model comprises organizational and system capabilities from a data management perspective. In contrast with the few existing research papers on EU-GDPR that treat selected aspects of the regulation, such as data breach notification or data portability, our study thereby provides an integrated perspective on enterprise-wide data management practices. The resulting capability model may also act as a classification framework for those studies that investigate specific aspects of the regulation.

The remainder of this paper is structured as follows: we first introduce the EU-GDPR as well as an overview of current research on the topic and on regulatory compliance in general. After outlining the research methodology and process, we motivate the capability perspective and present the capability model. We conclude by summarizing our contribution and discussing future research.

2 Background and related research

2.1 The European General Data Protection Regulation (EU-GDPR)

In January 2012, the European Commission published a proposal for an overhaul of data protection law within the European Union, which would become EU-GDPR[2]. It thereby addressed the need to remedy the fragmented implementations of the preceding Data Protection Directive (95/56/EC), as well as to account for the significant changes introduced by the internet and digital services [5], [6]. As a result, EU-GDPR directly applies in every EU member state. Moreover, any organization that processes personal data of EU-citizen must comply with it, regardless of the geographical location of their operations. If it fails to do so, fines with significantly heightened amounts will apply (i.e., up to 20 million euros or 4% of an organization's global revenues, whereas previous regulations averaged at ca. 500 000 euros). EU-GDPR reinforces existing concepts, and introduces new ones. Most notably, existing transparency mandates have been strengthened – organizations must now inform individuals about data processing in clear language and separately from general conditions, and are also required to present more granular consent options [5]. 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 (data breach notification). 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 as well as a right to oppose automated decision making [5]. All of these evolutions constitute a paradigm shift in data protection, towards greater choice and sovereignty for individuals, and more accountability for organizations [2], [6], [7].

2.2 EU-GDPR and Data Protection in IS Literature

Although EU-GDPR was finalized in 2016 and presents a major paradigm shift in data protection, it has attracted relatively little attention in IS literature so far. A query with the keyword "GDPR" returns 27 results on the AIS Electronic Library, as the time of writing (September 2018). The majority of these papers simply mention EU-GDPR, but only seven studies treat it as key topic. From Table 1, we see that existing EU-GDPR studies fall in the domains of information privacy practices (5 studies) and information privacy technologies and tools (2 studies), in [4]'s taxonomy of topic areas. However, with the exception of [14], all studies exclusively focus on one of EU-GDPR's requirements. There are two shortcomings in this approach: First, none of them is aimed at analyzing the entire regulation and its implication from an enterprise-wide perspective. Second, these papers do take the compliance requirements for granted and directly look into specific practices. Hence, we are still lacking a broader understanding

[2] Regulation (EU) 2016/679. Recitals (R.) and articles (art.) mentioned throughout the text refer to EU-GDPR unless otherwise specified.

of the challenges faced by companies in implementing EU-GDPR. [14] addresses this topic by proposing a Digital-Privacy Transformation "Gap-Map" that measures the organization's propensity for change. However, it exclusively takes a change management perspective, without investigating the compliance requirements and their implications on enterprise-wide data management practices.

Table 1. Summary of EU-GDPR-Related Studies in IS Literature

	Study type	**EU-GDPR aspects**	**Topic area based on [4]**	**Level of analysis**	**Research focus**
[9]	Empirical	Data breach notification	Information privacy practices	Orga-nisation	Applying data breach notification to past infringements
[10]	Conceptual	Data breach notification	Inf. privacy practices	Orga-nisation	Information security / incident management
[11]	Conceptual	Data portability	Information privacy impact	Market	Impacts of data portability right on competition dynamics
[12]	Conceptual	Privacy-by-design	Technologies and tools	Indivi–dual	Privacy label for GDPR
[13]	Conceptual	Tran-sparency	Technologies and tools	Orga–nisation	Guidelines for com-pliant privacy notices
[14]	Conceptual	Entire regulation	Impact / Inf. privacy practices*	Orga–nisation	Transformation framework for digital privacy
[8]	Empirical	Account-ability	Inf. privacy practices	Market	Review of third-party data processors
** scope beyond [4], covering organizational and individual readiness and transformation*					

2.3 Regulatory Compliance Management (RCM)

So far, the academic discussion on EU-GDPR has not linked up to the regulatory compliance management (RCM) research domain, although the latter could inform how to analyze regulations and their influence on business practice. RCM is defined as "ensuring that enterprises are structured and behave in accordance with the regulations that apply, i.e., with the guidelines specified in the regulations" [15]. RCM introduces useful background definitions to delimit relevant legal concepts. In his overview paper, [15] distinguishes between regulations (i.e., binding document), regulatory guidelines and compliance requirements, as provided in the legal text. Following interpretation, this ultimately results in concretized compliance requirements as implementation.

Two review papers from 2009 have analyzed the coverage of RCM in IS research. [16] conducted a literature analysis through the lens of enterprise architecture, and isolated 26 relevant papers. They found that while some aspects of RCM have been prominently studied (e.g. organizational and behavioral impacts of regulations, compliance supporting IT solutions), others had been neglected. Specifically, they found no contributions on the operationalization of compliance objectives. [17]'s literature analysis on RCM, revolves around the approaches (i.e., explanatory or

solution) and context (i.e., region, type and domain) of the considered contributions. From the 45 papers, the majority focused on North America, whereas only 3 of them focused on European issues. Related to data protection, they identified 2 papers that study Fair Information Practices, and only one on the European Data Protection Directive (95/46 EC), even though it had been enforced for 15 years. Furthermore, all identified contributions offered 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 that North America [17] and provide guidance to concretize strategic compliance objectives [16]. This last call is echoed by our literature review on EU-GDPR – although contributions exist around the topic, they all focus on specific aspects of the regulation, and lack a single integrating framework.

3 Research method

Given our stated goal to support companies in achieving EU-GDPR compliance, we adopt design science research (DSR) to develop a capability model, as an artefact "to solve identified organizational problems" [18]. Table 2 depicts the research steps, following the iterative process suggested by [19] and outlines the close interactions between academics and practitioners, comprising 5 focus group meetings with 33 data management experts from 22 companies and insights from 3 EU-GDPR projects.

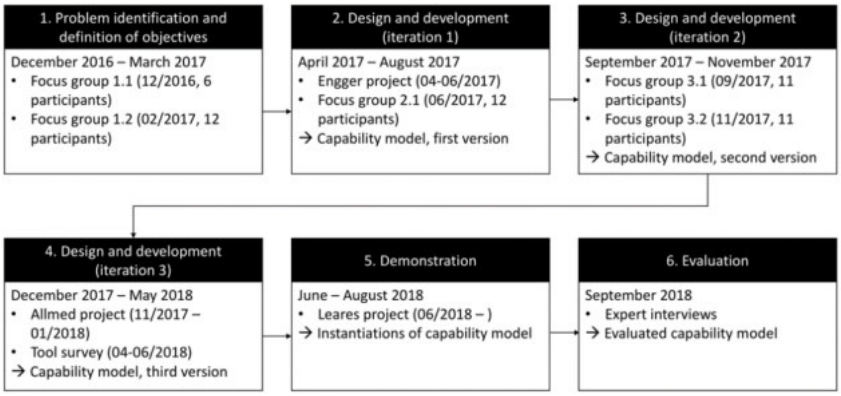

Figure 1. Research process (based on DSRM)

The **first phase** was meant to understand the problem at hand and specify the objectives of the solution to be developed. It was conducted between November 2016 and March 2017 based on an initial review of the regulation, with the objective of isolating requirements relevant for data management. We started by extracting and analyzing EU-GDPR's compliance requirements according to foundational data protection principles in legal literature (i.e. personal data, informational self-determination, accountability and transparency). To that end, we selected reference text books that

provide a comprehensive analysis of data protection foundations and applications – they integrate legal texts and their related preparatory works, as well as insights from case law and legal doctrine [20–22]. Early results of this analysis were discussed with practitioners through focus groups 1.1 and 1.2, allowing them to reflect on the regulation's impacts on their organizations and implementation challenges. These discussions led to an in-depth understanding of the issues in implementing EU-GDPR enterprise-wide and the subsequent decision to design a capability model.

The next phases (2, 3 and 4) were **iterative design cycles**, involving insights from field projects and internal research activities to design the capability model, as well as focus groups for collecting feedback. Internal research activities included a continuous analysis of EU-GDPR-specific legal literature [2], [5–7], [20], [22], [23], guidelines from official authorities [24–26] as well as interpretations from the private sector, including consortia (e.g. [27–30]) and industry stakeholders (e.g. [31]).

Phase 2, the first design iteration phase, comprised a project at Engger[3], a global engineering company, and resulted in the initial version of the capability model. It had just started a multi-project around EU-GDPR-compliant personal data aiming at harmonizing business partner data management in a highly distributed landscape, i.e., with around 500 systems in different countries and subsidiaries. This project helped understanding issues and define capabilities related to collection and distribution of personal data and consent. It ultimately led to the first version of the capability model that was presented to and discussed with data management experts in focus group 2.1.

During **phase 3**, the discussions in the two focus group meetings 3.1 and 3.2 revolved around the scope of the model. Feedback from focus group 3.1 indicated that security is usually a distinct function, and supported the need for a data management-centric perspective. 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. It was decided to set aside all security-related considerations from the capability model and focus exclusively on data management capabilities.

Phase 4 comprised a project around consent management at Allmed, a global pharmaceutical company. Its technical team had designed an MVP solution, which we analyzed based on the second version of the capability model. Insights from the project resulted in the capability model's third and final version. Afterwards, we analyzed software tools from major vendors claiming to support EU-GDPR compliance – to that end, we designed a taxonomy of desired functionalities based on the capability model (following the methodology proposed by [32]) and used it to classify 23 tools from major vendors. This analysis allowed us to validate the system capabilities.

Phases 5 and 6 included a demonstration with the EU-GDPR activities at Leares, a small consulting firm. The capability model proofed to be applicable and useful for assessing the current capabilities, identifying the required capabilities and prioritizing compliance activities. Additional expert interviews confirmed utility of the artefact.

[3] All company names have been anonymized.

4 Data Management Capabilities for EU-GDPR

4.1 Problem Formulation and Definition of Objectives

Discussions held in focus groups 1.1 and 1.2 revealed two main challenges with regards to GDPR compliance. First, participants recognized a lack of understanding of the regulation itself, while anticipating significant changes to the current way of storing and processing personal data on an enterprise-wide level. 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 vocabularies, which blocks the identification of feasible and compliant solutions and hinders progress. This led to the research objective of defining a capability model for EU-GDPR that assists data management professionals to understand and implement the regulation, as well as collaborate with legal colleagues.

4.2 Capabilities as a Link Towards Concretized Compliance Requirements

As theoretical foundation, we chose to rely on the RBV, as regulatory compliance is a component of firm performance, and contributes to an organization's control objectives (as defined by [33]). Building on [34]'s definition of an IT capability, we define data management capabilities for regulatory compliance as a firm's ability to acquire, deploy, and leverage its data resources in combination with other resources and capabilities in order to achieve an organization's compliance objectives.

Table 2. Positioning capabilities within RCM concepts

RCM concept	**Definition (based on [15])**	**Illustration in EU-GDPR**
Regulatory guideline	Stipulates a set of obligation to comply to.	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 / a specific condition to fulfill.	Extraction of requirements bearing data management relevance. E.g. art. 6 § 1 a and art. 7 § 1 require that data be processed according to individuals expressed consent.
Capability	*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 model, fulfilling its legal specification.	A concrete measure implemented in a specific organization to operationalize CRs. E.g. "In company X, consent data should be first recorded in system 1 and pushed to other systems every 12 hours".

The capability model complements RCM concepts [15] and acts as an abstraction layer between the normative aspects of the regulation, i.e. the regulatory guidelines and compliance requirements (CR), and the concretized compliance requirements (CCR), i.e. the concrete implementation of a CR. Introducing capabilities allows describing what organizations should do, as opposed to how they should do it, i.e. how the specific implementation should be carried out. Table 2 depicts this articulation.

4.3 Capability Model: Structure and Overview

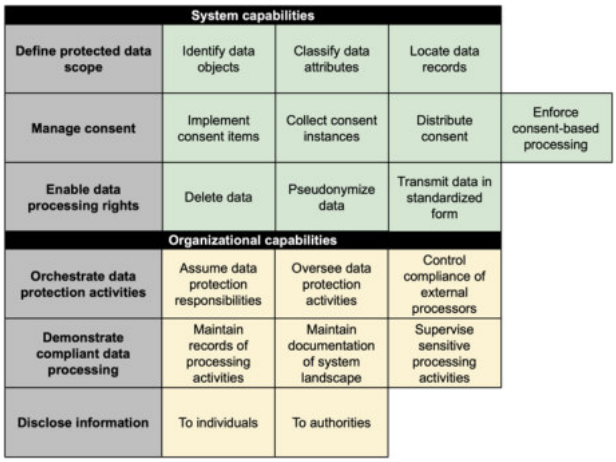

Figure 2. Capability model for data management in EU-GDPR

Art. 24 § 1 states the overall responsibility of organizations with regards to the regulation as the implementation of "appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with this Regulation". We thus derived our two main capability groups, i.e., system and organizational capabilities (see Figure 2), reflecting their predominant aspect[4]. Correspondingly, **system capabilities** are mainly enabled by data-processing systems, while **organizational capabilities** rely on data protection processes and responsibilities. Capabilities were derived from EU-GDPR's underlying principles, as described by legal literature, and reflect the "pillars" of the regulation. Sub-capabilities are the result of the analysis and express compliance requirements. In the following sections, we present each of the suggested capabilities, along with its justification, the empirical evidence and the sub-capabilities.

Define Protected Data Scope. 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,

[4] In the RBV, capabilities "involve complex patterns of coordination between people and between people and other resources" [35]. Authors relying on the RBV in the IS literature usually demarcate technological and organizational aspects that underpin IS capabilities [36, 37].

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" [21].

Focus groups 1.1 and 1.2 indicated that companies generally had no overview on the personal data collected and used during processes, especially in terms of storage location. A participant of focus group 3.2 asked: "How do you identify personal data in a heterogeneous IT-System landscape?" Follow-up questions revolved around means to identify personal data. The project at Engger provided significant insight regarding this capability group. One of its main objectives was making sure that personal data was consistently kept up-to-date within all systems, which proved difficult due to multiple overlapping systems managed in independent subsidiaries. Overall, companies faced two main challenges: determining what kind of personal data they were processing, and where such data was stored. The resulting capability may be best summarized by [20], stating that "organizations must have perfect knowledge of personal data". Practitioner reports also fall in line with this statement – [29] recommend two actions that mirror these issues (e.g. data discovery and system mapping) and suggest that personal data should not only be identified, but also classified. This is required as EU-GDPR prescribes higher protection levels for data that is considered sensitive (R. 51). The resulting sub-capabilities are:

- **Identify data objects:** identify data domains and related data objects that fall within EU-GDPR's scope of applicability.
- **Classify data attributes:** assign levels of sensitivity to data attributes contained within personal data objects.
- **Locate data records:** identify all storage instances of personal data objects and have the ability to access and retrieve them.

Manage Consent. This capability comprises the prerequisites for collecting consent and ensuring consent-based processing of information. The principle of consent [5], [20, pp. 12, 94], [22, p. 93] is arguably one of the pivotal concepts of EU-GDPR and an expression of the right to informational self-determination. It can be defined as ability for each individual to determine whether and to what ends information about themselves can be processed [6]. The related concepts of conditionality, granularity and specificity are the most challenging for data management [24]. Conditionality (art. 7 § 4) means that consent for processing activities cannot be bundled in general conditions, and that a difference should be made between necessary and optional processing activities for a given purpose. Granularity (R. 43) 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). This is a departure from practices before GDPR, when consent was mostly obtained through the bulk acceptance of general conditions.

Consent management found a significant echo in our focus groups. During focus group 3.1, none of the participants reported solutions either in final stages nor operational. During focus group 3.2, more questions were asked regarding consent management than all other capabilities combined. The Allmed project goal was making

consent information accessible and readable by all systems, which mirror capabilities "distribute consent" and "enforce consent-based processing". However, difficulties arouse in two areas. First, the system would need to be connected to every system storing and processing personal data – identification of 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 unstructured form (e.g. within general conditions, contracts, webpages). A specific sub-capability was added to reflect this issue, and is a prerequisite to all other consent-related capabilities. The resulting sub-capabilities are:

- **Implement consent items:** define and implement consent items that mirror data processing activities performed throughout business processes.
- **Record consent instances:** collect and record consent expressed by individuals.
- **Distribute consent:** ensure consent items updates in all affected processing systems.
- **Enforce consent-based processing:** ensure that data processing activities are performed in accordance with consent expressed by individuals.

Enable Data Processing Rights. This capability denotes the ability to process data according to 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 [5], [20, p. 12], [22, pp. 31, 38].
Art. 17 provisions a "right of erasure", according to which individuals can request that organizations delete their personal data (provided that they have no other obligation to keep said data). From a technical perspective, enterprise systems usually prevent users from deleting data and practitioners expressed a difficulty in that regard. When asked about it, none of the participants of focus group 3.1 reported that they had operational deletion processes or mechanisms. Focus group 3.2 also expressed a lack of well-established solutions at this level, and our tool study identified only 2 solutions supporting this capability. Art. 25 mandates privacy by design / by default approaches, including the principle of minimization [22, p. 90], i.e. processing as little personal data as possible. One way of operationalizing it is pseudonymization, which is a rare occurrence of EU-GDPR mentioning a specific technological approach (R. 28-29). This can be seen as an alternative to deletion, as pseudonymized data exits EU-GDPR's scope of applicability, and was thus added as second order capability. Art. 20 introduces a "right do 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. During focus group 3.1, only a quarter of respondents declared that the provision of data in standardized formats was mature, and none of them reported working communication channels. We have identified only two solutions in our tool study, both of which are marketed as "Customer Identity and Access Management Systems" (CIAM). The resulting sub-capabilities are:

- **Delete data:** permanently remove data records from their systems.
- **Pseudonymize data:** use pseudonymization techniques in order to adhere to the principle of minimization.

- **Transmit data in standardized form:** transmit personal data to external parties using standard formats and set up communication channels with other organizations.

Orchestrate Data Protection Activities. 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 [5], [20, p. 12], [22, pp. 31, 53, 71]. As stated, focus group feedback indicated that data managers often are at a loss as of who to 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, they did not have a clearly designated contact person. On several occasions, responsibilities (e.g., for 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 acquiring an overview of processing activities, serve as advisory contact person [25], oversee record keeping and cooperation with authorities. We designed related capabilities for data protection oversight.

EU-GDPR also 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 – the use of cloud services also falls into this situation, 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, websites) for the storage and processing of data. A corresponding capability was therefore added. The resulting sub-capabilities are:

- **Assume data protection responsibilities:** responsibilities for data protection-related tasks in all business functions that routinely process personal data.
- **Oversee data protection activities:** a leading role should oversee, organize, control and coordinate data protection activities.
- **Control compliance of external processors:** monitor that data processing conducted by third parties for EU-GDPR compliance.

Demonstrate Compliant Data Processing. This capability comprises the ability to record and evaluate sensitive processing activities, as well as to document system landscapes. It was derived from the documentation component of the principle of accountability [5], [22, p. 44]. 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 [30], and all participants of focus group 3.2 acknowledged that documentation represented a significant effort. Maintaining system landscape documentation was identified as another sub-capability, as focus groups indicate that most organizations have difficulties locating data – this was the very motivation for the Engger project, and one significant roadblock for Allmed's solution implementation. Art. 35-36 further require organizations to conduct and document in-depth data protection impact assessments (DPIA) when performing sensitive processing activities. The resulting sub-capabilities are:

- **Maintain records of processing activities:** inventory and document personal data-related activities performed throughout business processes.
- **Maintain documentation of system landscape:** inventory and document systems that store and process personal data on a regular basis.
- **Supervise sensitive processing activities:** identify and evaluate sensitive data processing activities.

Disclose Information. This capability involves the ability to disclose information to individuals (R. 58) and authorities (art. 31). It was derived from the principle of trans–parency, which requests data protection measures to be clearly exposed [5], [20, p. 17].

Transparency requirements apply in two cases [26]. First, at the point of data collection, organizations must present related information separately, in a manner (e.g., language, illustrations) that can be easily comprehended. This would include, for instance, a clear description of each consent item. Transparency also refers to communications with individuals after data is collected, when organizations are faced with right-related requests (e.g., access, rectification, deletion). 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 the ability to present relevant information / documentation as proof of compliance.

These capabilities may be seen as the operationalization of the principle of accountability, which is materialized by documentation. Since such documentation should contain all relevant information regarding an organization's data protection practices, these capabilities are about presenting that information to the interested parties (i.e. individuals and authorities). The resulting sub-capabilities are:

- **Disclose information to individuals:** provide individuals with complete and understandable information regarding the processing of their personal data and respond to their data protection-related requests.
- **Disclose information to authorities:** collaborate with designated data protection authorities and communicate relevant information upon request.

4.4 Demonstration

The main purpose of the capability model is to guide organizations in implementing EU-GDPR's requirements into their existing practices. To demonstrate its applicability and usefulness in EU-GDPR initiatives, we present how it was applied to assess the situation of Leares, a small-sized consulting firm that had started to draft a GDPR "action plan". A lengthy to-do list compiled 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. There were significant shortcomings with this approach. First, there was no indication of why certain actions were necessary, or what compliance issue they were meant to fix. Second, actions were presented as isolated, one-time efforts – there was no indication as to what extent GDPR compliance was actually achieved, or how it would be maintained in the future. Third, and most

notably, these action items focused mostly on technical issues, with no documentation mechanisms or compliance processes put in place.

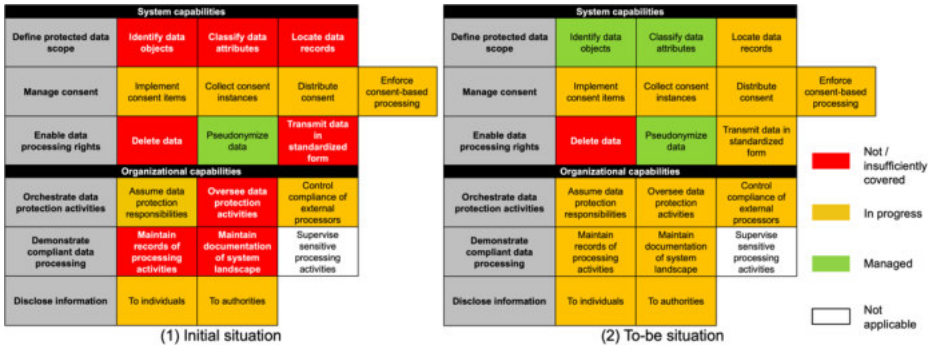

Figure 3. Evaluation of Leares' compliance level

Using the capability model contributed to alleviate these issues and helped Leares in identifying compliance gaps as well as defining and prioritizing actions. Going through the model, we were able to assign each check-list activity to capabilities, and assess 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 these cases, new measures had to be defined. The instantiations depicted in Figure 3 show how the model was used to assess existing practices in the initial situation, along with a realistic target situation to be achieved within the next months. As a result of using the capability model, Leares was able to devise a structured action plan, covering all aspects of its data management practices.

5 Conclusion and Outlook

This paper introduces a data management perspective to EU-GDPR and argues that the regulation requires companies to build a dedicated data management capability. The suggested capability model was developed in an iterative design science process, integrating both interpretation of legal texts and practical insights from focus groups with more than 30 experts and from 3 EU-GDPR projects. By translating compliance requirements into organizational and system capabilities, it contributes to (1) building common ground between legal and data management domains and (2) assisting organizations in assessing practices, identifying and deciding on implementation options for achieving compliance with EU-GDPR. From a research perspective, our capability model complements the emerging body of research on EU-GDPR, that mostly investigates selected information privacy practices. The capability model may be used to classify and integrate these focused research efforts into an enterprise-wide perspective. Furthermore, it complements IS security research by focusing on non-security aspects of information privacy. For practice, the capability model supports

companies in developing a systematic approach towards achieving EU-GDPR compliance and monitoring progress, instead of "fire-fighting". As outlook for future research, our focus group discussions reveal that implementing EU-GDPR is not a one-time effort, but an ongoing process. The suggested capability model may serve as a basis for studying how the capabilities are being built and how they can be assessed. As it is supposed to contribute to reaching a firm's control objective, a potential lead for further research would be to propose indicators of compliance goals and measure them.

Acknowledgements

This research was supported by the Competence Center Corporate Data Quality (CC CDQ). The authors would like to thank the experts that contributed to this research.

References

1. The Economist: The World's Most Valuable Resource Is No Longer Oil, But Data, (2017).
2. De Hert, P., Papakonstantinou, V.: The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. Computer Law & Security Review. 28, 130–142 (2012).
3. The Race to GDPR: A Study of Companies in the United States & Europe. Ponemon Institute (2018).
4. Bélanger, F., Crossler, R.E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly. 35, 1017–1042 (2011).
5. Nicolaidou, I.L., Georgiades, C.: The GDPR: New Horizons. In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 3–18. Springer International Publishing, Cham (2017).
6. Mitrou, L.: The General Data Protection Regulation: A Law for the Digital Age? In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 19–57. Springer International Publishing, Cham (2017).
7. De Hert, P., Papakonstantinou, V.: The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? Computer Law & Security Review. 32, 179–194 (2016).
8. Kurtz, C., Semmann, M., Böhmann, T.: Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. In: AMCIS 2018 Proceedings (2018).
9. Petkov, P., Helfert, M.: Identifying Emerging Challenges for ICT industry in Ireland: Multiple Case Study Analysis of Data Privacy Breaches. In: AMCIS 2017 Proceedings (2017).
10. Karyda, M., Mitrou, L.: Data Breach Notification: Issues and Challenges for Security Management. In: MCIS 2016 Proceedings (2016).
11. Engels, B.: Data Portability and Online Platforms The Effects on Competition. In: BLED 2016 Proceedings. pp. 19–22 (2016).
12. Alboaie, L.: Towards a Smart Society through Personal Assistants Employing Executable Choreographies. In: ISD 2017 Proceedings (2017).
13. Fox, G., Tonge, C., Lynn, T., Mooney, J.: Communicating Compliance: Developing a GDPR Privacy Label. In: AMCIS 2018 Proceedings (2018).
14. Russell, K.D., O'Raghallaigh, P., O'Reilly, P., Hayes, J.: Digital Privacy GDPR: A Proposed Digital Transformation Framework. In: AMCIS 2018 Proceedings (2018).
15. El Kharbili, M.: Business Process Regulatory Compliance Management Solution Frameworks: A Comparative Evaluation. In: APCCM 2012 Proceedings. pp. 23–32 (2012).

16. Cleven, A., Winter, R.: Regulatory Compliance in Information Systems Research - Literature Analysis and Research Agenda. In: Enterprise, Business Process and Information Systems Modeling. pp. 174–186. Springer-Verlag, Berlin, Heidelberg (2009).
17. Abdullah, N.S., Indulska, M., Shazia, S.: A Study of Compliance Management in Information Systems Research. In: ECIS 2009 Proceedings. pp. 1–10 (2009).
18. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly. 28, 75–105 (2004).
19. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24, 45–77 (2007).
20. Bensoussan, A., Avignon, C., Bensoussan-Brulé, V., Forster, F., Torres, C.: Règlement Européen sur la Protection des Données: Textes, Commentaires et Orientations Pratiques. Bruylant, Brussels (2018).
21. Debet, A., Massot, J., Métallinos, N.: Informatique et libertés: la protection des données à caractère personnel en droit français et européen. Lextenso, Issy-les-Moulineaux (2015).
22. Voigt, P., Von Dem Bussche, A.: The EU general data protection regulation (GDPR): A Practical Guide. Springer International Publishing, Cham (2017).
23. Guadamuz, A.: Developing a Right to be Forgotten. In: Synodinou, T.-E., Jougleux, P., Markou, C., and Prastitou, T. (eds.) EU Internet Law: Regulation and Enforcement. pp. 59–76. Springer International Publishing, Cham (2017).
24. European Data Protection Board: Guidelines On Consent Under Regulation 2016/679 (WP259, rev.01). EDPB (2018).
25. European Data Protection Board: Guidelines on Data Protection Officers (WP243 rev.01). EDPB (2017).
26. European Data Protection Board: Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01). EDPB (2018).
27. Iannopollo, E., Balaouras, S., Harrison, P.: The Five Milestones to GDPR Success. Forrester Research (2017).
28. Merlivat, S., Iannopollo, E., Parrish, M., Khatibloo, F., Oesterreich, M., Liu, S., Turley, C.: Digital Advertising under GDPR Hinges on Data Management. Forrester Research (2017).
29. Peyret, H., Cullen, A., McKinnon, C., Blissent, J., Iannopollo, E., Kramer, A., Lynch, D.: Enhance your Data Governance to Meet New Privacy Mandates. Forrester Research (2017).
30. Iannopollo, E., Balaouras, S., Pikulik, E., Dostie, P.: The State of GDPR Readiness. Forrester Research (2018).
31. Deutsche Telekom: Binding Interpretations: General Data Protection Regulation (GDPR). Deutsche Telekom (2016).
32. Nickerson, R.C., Varshney, U., Muntermann, J.: A Method for Taxonomy Development and Its Application in Information Systems. European Journal of Information Systems. 22, 336–359 (2013).
33. Sadiq, S., Governatori, G., Namiri, K.: Modeling Control Objectives for Business Process Compliance. In: Alonso, G., Dadam, P., and Rosemann, M. (eds.) BPM 2007 Proceedings. pp. 149–164. Springer-Verlag, Berlin, Heidelberg (2007).
34. Zhang, M., Sarker, S., Sarker, S.: Drivers and Export Performance Impacts of IT Capability in 'Born-Global' Firms: a Cross-national Study. Information Systems Journal. 23, 419–443 (2013).
35. Grant, R.M.: The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation. California Management Review. 33, 114 (1991).
36. Baiyere, A., Salmela, H.: Towards a Unified View of Information System (IS) Capability. In: PACIS 2014 Proceedings (2014).
37. Bharadwaj, A.: A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. MIS Quarterly. 24, 169–196 (2000).