Personal data management inside and out

Integrating data protection requirements in the data life cycle

Clément Labadie*,[a], Christine Legner[a]

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

Abstract. *Personal data is increasingly positioned as a valuable asset. While individuals generate and expose ever-expanding volumes of personal information online, certain tech companies have built their business models on the personal data they gather. In this context, lawmakers are revising data protection regulations in order to provide individuals with enhanced rights and set new rules regarding the way corporations collect, manage, and share personal information. We argue that recent data protection regulatory frameworks such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) are fundamentally about data management. Yet, there have been no attempts to analyze the regulations in terms of their implications on the data life cycle. In this paper, we systematically analyze the GDPR and the CCPA, and identify their implications on the data life cycle. To synthesize our findings, we propose a semi-formal notation of the resulting changes on the personal data life cycle, in the form of a process and data model governed by business rules, consolidated in a reference personal data life cycle model for data protection. To the best of our knowledge, this study represents one of the first attempts to provide a data-centric view on data protection regulatory requirements.*

Keywords. Data life cycle • Data protection • Personal data • Regulatory compliance

Communicated by Agnes Koschmider. Received 2019-12-15. Accepted after 2 revisions on 2020-05-20.

1 Introduction

The idea of a right to privacy is not a novel one - in the 19th century, the attorney Samuel Warren and the lawyer Louis Brandeis described a "right to be left alone" (Warren and Brandeis 1890). Organizations' ever-enhancing ability to acquire and process personal data makes this increasingly relevant in our current reality. Through customer relationship management (CRM), personal data has become of strategic relevance for enterprises to improve interactions with their customers and create mutual benefits (Payne and Frow 2005). As individuals generate and expose ever-expanding volumes of personal information online, "digital native" enterprises assemble individualized profiles to target consumers and deliver personalized content and services. In fact, personal information processing is the very foundation of some of the last decade's most successful corporations. From a privacy perspective, this leads to a redefined threat landscape. When it comes to data, the idea of misuse traditionally refers to security concepts and expresses the risk of unauthorized access, meaning that a malevolent, external party might access data. The increasing scope of personal data processing has also enlightened a new threat: that of "unintended inferences" (Burt 2019), which occurs when a rightful custodian of personal data uses it for unauthorized purposes.

Addressing this threat is the objective of all data protection regulations, and it is no surprise that they started appearing in Europe in the early

* Corresponding author.
E-mail. clement.labadie@unil.ch
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.

1980s, following the widespread adoption of information systems in enterprises (Hirschheim and Klein 2012). Having been introduced before the democratization of the internet, these regulations needed to be substantially revisited to cope with the exploitation of personal information by certain tech companies. This was the motivation for major revisions of data protection regulations (Mitrou 2017; Nicolaidou and Georgiades 2017), such as the European Union's General Data Protection Regulation (GDPR- European Parliament and Council of the European Union (2016)), and the State of California's Consumer Privacy Protection Act (CCPA- California State Senate (2018)).

While these regulations aim to impose restrictions on corporate behaviors, they are fundamentally about data management, bearing technical as well as organizational impact for data management organizations (Hakim et al. 2018). They introduce data-related rights and data transparency requirements (both internal and external) that force organizations to substantially rework their data management practices. To comply with emerging data protection regulations, organizations must gain a precise overview of and change the way they manage personal data from beginning (gathering) to end (archiving or even deletion).

Over the years, in research as well as practice, data-centric life cycle models have been developed with this objective in mind, of which the model built by Levitin and Redman (1993) was one of the first. These models describe all necessary steps to manage data elements form start to finish. They stem from a variety of domains and address diverse data types (e. g. product data, scientific/research data), but very few are applicable to personal data. When such models consider privacy aspects at all, the information is usually derived from non-legal definitions of privacy and is not aligned with the precise legal requirements. Similarly, privacy research in IS has not focused on regulatory matters (Bélanger and Crossler 2011) and neither has customer relationship management or consumer research. Based on this observation, this paper addresses two research questions (RQs):

- RQ 1: What is the impact of data protection regulations on the personal data life cycle?
- RQ 2: How could data life cycle models be amended in order to address regulatory requirements for data protection?

To address RQ 1, we analyze two recent data protection regulation frameworks (the GDPR and the CCPA). We find that these requirements directly impact the way data objects are created, processed, and maintained. From our analysis, we propose a classification of legal requirements from data protection legislation and show how they impact the data life cycle stages.

As an answer to RQ 2, we propose a reference personal data life cycle model for data protection, which comprises a data life cycle notation for data protection, outlining how general data management activities and steps are impacted by the aforementioned regulations. The notation is complemented by data model extensions to capture compliance-relevant attributes, as well as business rules to operationalize the life cycle process.

We start the detailed content by presenting perspectives on the regulatory context and the notion of personal data and reviewing existing research related to data protection and the data life cycle. We then outline our research methodology and process. Finally, we present a classification of legal requirements and derive a data life cycle notation with process and data models, as well as related business rules. We conclude with a summary and outlook on future research.

2 Background

2.1 Data protection regulatory landscape

Since May 25, 2018, the GDPR directly applies to every European Union (EU) member state (Art. 99), repealing the preceding Data Protection Directive (95/56/EC, Art. 94). It addresses the need to remedy the fragmented implementations of the Data Protection Directive and accounts for the significant changes introduced by the mainstream adoption of the internet and the digital transformation (Mitrou 2017; Nicolaidou and Georgiades

2017). Any organization that processes EU citizens' personal data must comply with it, regardless of its geographical location. Violations are punishable by substantially higher fines (up to 20 million euros or 4% of an organization's global revenue, when previous regulations averaged about 500,000 euros). The GDPR constitutes a landmark regulation for data protection in the EU and similar regulations are being introduced in other parts of the world. In Europe, Switzerland is currently undergoing an overhaul of its data protection legal framework – after several delays, it is set to be enforced in the beginning of 2022 and is expected to incorporate the measures the GDPR (Métille and Raedler 2017) introduced. In 2017, China introduced its cyber security legislation, which covers data protection aspects such as personal information protection and rules for transnational data transmission. In 2018, following a supreme court judgment that declared privacy a fundamental right, India introduced a draft for a Personal Data Protection Bill (Parliament of the Republic of India 2018), with the objective of acting as a reference template for developing countries to introduce similar regulations (Palanisamy and Nandle 2018). The United States of America still does not have a single, general data protection regulation. Instead, several sector-specific laws co-exist, such as the Children's Online Privacy Protection Rule, the Federal Privacy Act (which only applies to federal agencies), and HIPAA (introduced in 1996, it contains requirements similar to the GDPR 's, but is restricted to health-related data). Since the Facebook-Cambridge Analytica data scandal of 2018, there have been calls for a federal GDPR-inspired data protection regulation (Rubio 2019). So far, only the state of California has passed its own GDPR-inspired data protection law (California State Senate 2018), which became effective on January 1, 2020.

Although these regulations originate from different legislative bodies, they all address the same issues, and some are directly inspired by the GDPR. Therefore, even if their requirements are positioned at differing levels of severity, the underlying concepts (such as personal data, data processing, consent, organizational and technical measures, and processes) remain the same, allowing for comparisons. Most importantly, existing transparency mandates have been strengthened. Organizations must now inform individuals about data processing in clear language and separately from general conditions, at the point of data collection. This means that organizations must define processing purposes for collected data elements before they gather such data. In the GDPR, they are additionally required to present granular consent options as opt-in for non-mandatory processing activities. Both the GDPR and the CCPA introduce the concept of accountability, which prompts organizations to be able to demonstrate compliance with the regulation. As they process data, they must also operationalize data rights, referring to access, rectification and restriction. When processing is no longer necessary or desired, individuals may request that their data records be deleted from enterprise systems.

2.2 Defining personal data

From a regulatory perspective, personal data can be 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" (Debet et al. 2015). In practice, most companies collect personal data about their customers, and it is often referred to as consumer or customer data. In that regard, it can be defined as "a set of data that represents and is associated with the identity, activities and service offering associated with a unique individual" (Tapsell et al. 2018). The aspect of service offering is prevalent in the consumer/customer data literature and has been emphasized in the broader customer relationship management (CRM) field. In CRM, customer data is considered as an opportunity to understand the customer and co-create customer value (Payne and Frow 2005). The related contributions focus on collecting, organizing,

and using customer data in order to build long-term relationships with customers (Saarijärvi et al. 2015). In this study, we consider personal data as data that contains personally identifiable information, meaning that it identifies a specific individual and/or provides information about them.

2.3 Data life cycle management

In order to reflect the changes in data management practices induced by recent data protection regulation frameworks, this study uses the data life cycle as a frame of reference. On a high level of abstraction, "the life cycle of something [. . .] is the series of developments that take place in it from its beginning until the end of its usefulness" (Collins English Dictionary 2019). The life cycle concept has been applied to various data-related domains (e. g. product data, scientific/research data) and has enjoyed a renewed interest in the context of big and open data landscapes. Four overview studies provide a comprehensive analysis and synthesis of the data life cycle and will be summarized in the next paragraphs. Out of the multitude of data life cycle models covered, we have identified only one that specifically deals with personal data.

Möller (2013) conducted an extensive meta-analysis of life cycle models to derive the Abstract Data Lifecycle Model (ADLC) for the semantic web. He reviewed life cycle models from media production, e-learning, digital libraries, knowledge and content management and databases – the last two are the ones closest to our research field. In the database domain, the data life cycle is often associated with four basic operations of persistent storage known as CRUD (create, read, update, and delete - Möller 2013). In the knowledge and content management domain, which represents the largest subset in Möller (2013)'s study, seven models outline the steps that enable organizations to capture implicit knowledge, structure it in a way that fits the need of the target audience, and maintain it as it evolves. These models put an emphasis on ontology development (Staab et al. 2001), roles, processes and tools for metadata generation (Greenberg 2003), web content management systems (McKeever 2003), digital curation (Higgins 2008) and semantic applications (Modritscher 2009), among others. They put an emphasis on data creation/authoring, distribution, maintenance, and preservation, but do not specifically target personal data. These steps, especially the latter, are not highly relevant with regards to personal data, in the sense that the data is generally collected "as is" and is not the result of a dedicated creation/authorship process. Furthermore, the preservation aspect contradicts legal requirements that emphasize data deletion.

In the same year, Ofner et al. (2013) proposed a framework for data life cycle models in the context of master data management. Although the study approaches the topic from a product data point of view, the authors surveyed general life cycle models in the master data domain. One of them (Levitin and Redman 1993) puts the data life cycle in three main activity clusters: the acquisition cycle, the usage cycle, and assessment activities that intervene in both cycles, and include data deletion. This perspective is aligned with data protection, and the argument can be made that all life cycle models, regardless of the domain, can be described according to this structure. This also holds true for the general steps the professional association DAMA International (2009) outlined which additionally suggest that "when effectively managed, the data lifecycle begins even before data acquisition, with enterprise planning for data, specification of data and enablement of data capture, delivery, storage, and controls." This perspective is in line with informational duties prescribed by data protection regulations.

The studies by Sinaeepourfard et al. (2016b) and Sinaeepourfard et al. (2016a) present a meta-analysis of 17 data life cycle models. They stem from a variety of domains and there is a significant overlap with those Möller (2013) and Ofner et al. (2013) analyzed. According to Sinaeepourfard et al. (2016a), the observed large number and topical variety of data life cycle models can be explained by the fact that they are meant to address the specific requirements of a particular field, which is not aligned to the authors' goal of establishing a "scenario-agnostic" model.

Among this abundant literature, we found only one data life cycle model that specifically addresses personal data management (Alshammari and Simpson 2018). It is based on the ADLC model Möller (2013) proposed and uses the Global Privacy Standard as reference to incorporate privacy by design aspects into the data life cycle. Although it specifically mentions the GDPR, the authors approach the topic through a wider set of principles to prevent limiting the scope of their model to a specific regulatory framework. The study elaborates on the various roles involved in the life cycle stages and describes the associated activities and dependencies in terms of input and output. It also explains the steps through a concrete case study. This contribution is much closer to our research objective, although it is not meant to express regulatory requirements.

2.4 Research motivation

We can summarize the literature as follows. First, we observe an increasing number of data protection regulations that build on similar concepts and seek to extend data protection requirements toward increased transparency and control for individuals. Implementing these requirements prompts companies to revise data management practices.

Second, prior research on personal data management mostly focuses on customer/consumer data and does so either from a CRM perspective, or investigates the non-legal aspects of privacy.

Third, the data life cycle research domain is a prolific one and comprises a large number of domain-specific contributions, as well as a few attempting to generalize life cycle concepts. Among these contributions, only one data life cycle model addresses the topic of personal data. However, even though it mentions the GDPR as exemplary motivation, it does not formally integrate a regulatory compliance point of view.

To address this gap in the literature, our study contributes a regulation-focused and data-centric approach to personal data management by analyzing and expressing data protection regulatory requirements in the data life cycle, and proposing data objects, attributes, and business rules to operationalize data life cycle steps. We adopt an end-to-end lens on the data life cycle, with a starting point prior to data collection. In that sense, our approach constitutes an answer to the call for data protection by design and by default formulated in the GDPR (Art. 25).

Our data-centric focus means that we have excluded other aspects of data protection regulations. We do not cover organizational requirements such as appointing a data protection officer or adopting a code of conduct. We also do not address information security requirements, which are related to a different research domain, and are generally addressed separately in practice.

3 Research approach

In order to develop the data life cycle model in a rigorous scientific research process, we follow the established design science research guidelines (Hevner et al. 2004) and the methodological steps Peffers et al. (2007) suggested. As depicted in Fig. 1, our research process comprised three design iterations and involved four focus group meetings. These focus groups were held with more than 25 data management experts from 20 multinational organizations. Each focus group lasted approximately two hours and focused on either problem identification (Focus groups 1 and 2) or evaluating different versions of the artifact (Focus groups 3 and 4).

During the first step, we analyzed the implementation challenges induced by data protection regulations. For this purpose, we analyzed the complete GDPR regulations, based on foundational data protection principles. Our primary sources consisted of legal textbooks (Bensoussan et al. 2018; Debet et al. 2015; Meier 2011; Voigt and Von Dem Bussche 2017). We then discussed the GDPR's requirements with experienced practitioners in Focus groups 1 and 2 and collected questions as well information about implementation challenges or difficulties in their organizations. This resulted in the observation that regulatory requirements are formulated in a way that does not immediately translate in data management terms.

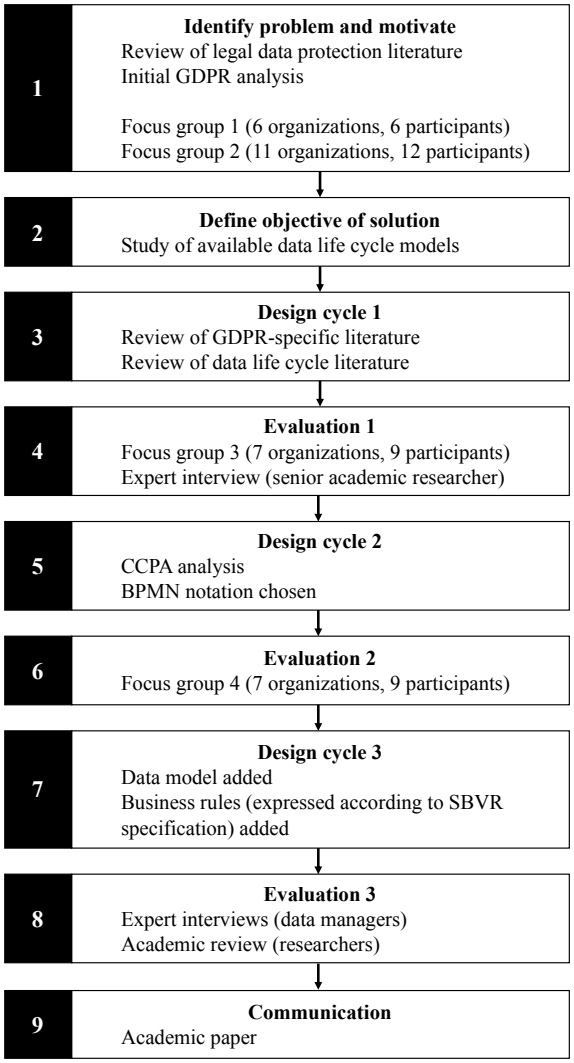

Figure 1: Research process

As a result, practitioners were unsure of the impact of such requirements on their activities.

During the second step, we determined the objectives of our study. To address the gaps identified in the first phase, we set out to develop a data life cycle model for the specific purpose of representing data protection regulatory requirements.

The third step consisted of the first design cycle. To develop the data life cycle model, we analyzed legal literature that is focused on the GDPR in order to derive key principles that underpin the emerging regulations. We then analyzed the GDPR according to these principles and extracted requirements that impact data management. For this purpose, we looked into GDPR-specific literature (De Hert and Papakonstantinou 2012, 2016; Guadamuz 2017; Mitrou 2017; Nicolaidou and Georgiades 2017; Tikkinen-Piri et al. 2018) as well as guidelines from official authorities (Commission Nationale de l'Informatique et des Libertés 2018; European Data Protection Board 2018a,b).

We then conducted a literature review on data life cycle models. This enabled us to understand the typical articulation of data life cycle steps, and to confirm that existing models did not account for the specific requirements imposed by data protection regulations. Based on this review, we designed a first iteration of our data life cycle model, which extended existing models by amending and adding steps.

In a fourth step, our proposed model was evaluated through the third focus group with nine practitioners from seven organizations. Participants confirmed the general structure and commented on the consistency of the model (specifically, the order in which to position one of the newly designed steps), as well as on its level of detail. We also gathered concrete difficulties and roadblocks participants encountered along each life cycle step.

The fifth step consisted of the second design cycle, and we included the CCPA in our analysis of legal requirements in the light of the foundational principles identified during the first step. In parallel, we proceeded to rework our data life cycle model, based on the feedback. At this stage, BPMN was chosen as a reference notation, and the data life cycle reference model was redesigned accordingly.

In a sixth step, the redesigned data life cycle model was evaluated by means of an expert interview with a senior information systems researcher with knowledge of privacy and compliance topics. Additionally, we used a questionnaire distributed during Focus group 4 (with nine participants from seven organizations). We selected relevant evaluation criteria as described by Prat et al. (2015) with regards to the model's structure (criteria: fidelity to modeled phenomenon, simplicity, completeness, and consistency) and fit to the target

audience's environment (criteria: usefulness and ease of use). Our expert, as well as focus group participants, agreed that the proposed model was valid (accurately depicting data protection legal requirements), had an appropriate level of detail, consistent steps, and was easy to understand. In fact, these dimensions received evaluation scores of 4 and above (with 2 holdouts for the fidelity criterion). However, we observed lower scores with regards to the simplicity and usefulness of the model, with a consensus at around 3 out of 5, and one 2 out of 5. In their comments, participants noted that the model did not provide sufficient guidance about how to handle these steps in practice, especially on a technical level. Examples of remarks from the evaluation questionnaire included the following:

- "Detailed model is more tangible and sophisticated."
- "Provide a pragmatic proposal – how to manage it in reality."
- "Elaborate on details, e. g. rules, technical handling, etc."
- "Propose a business data model with the whole meta-data management in it, including end-of-life information."

To alleviate these concerns, the seventh phase consisted of an additional design cycle to enrich the data life cycle model with a simple, compliance-oriented data model, containing data elements (objects and attributes) that need to be recorded in order to operationalize the proposed steps on a technical level. The data model is supported by business rules that were designed following the Semantics of Business Vocabulary and Business Rules (SBVR) standard. A set of structural business rules specify the content of data objects in the data model, and a set of operational business rules steer the life cycle process and specify data operations throughout process steps, using the CRUD set of operations.

The eighth step consisted of an evaluation of the data model and business rules, by means of three expert interviews with representatives of two multinational organizations, as well as researcher feedback form the academic review. At this stage, we sought to guarantee the understandability, completeness, consistency, and effectiveness of the models and business rules (Prat et al. 2015). In addition, we evaluated the adequacy, usefulness, and applicability of the overall approach, referring to the combination of the life cycle model, data model, and business rules taken together. These evaluations were carried out as semi-structured interviews, and questions were evaluated based on a 5-level Likert scale. The experts consisted of a data architect and a data community manager from an organization active in the life-sciences industry, as well as a data architect from an organization active in the fashion & jewelry industry. All of them have over ten years of experience in the data management domain. The experts viewed the overall approach, data model, and business rules positively - their average rating of each dimension was above 3 (5 indicating full agreement) for all criteria except one.

Specifically, the data life cycle model's (s. Fig. 3) ability to show the impact of data protection regulations on data management activities was rated with 4 out of 5 by all experts. The understandability, completeness, consistency and efficacy of the data model and business rules in the onboarding and usage phase were all rated with a minimum of 4 out of 5. Regarding the business rules for the end-of-life phase, two of the experts rated all criteria with a minimum of 4. One of them agreed that they were understandable and consistent (4 out of 5), but questioned their completeness and, as a result, efficacy. We made minor adjustments to the model to account for this feedback.

Following comments from academic reviewers, we also amended the data life cycle model to better reflect the GDPR's right to restriction (art. 18) and breach notification requirement (art. 33). In order to maintain consistency with the updated data life cycle model, attributes registering the provenance of personal data and its recipients for a given processing purpose were added to the data model.

This paper constitutes the ninth and final step.

4 Integrating data protection requirements in the data life cycle

4.1 Data life cycle for personal data

In order to analyze the way data protection requirements impact the data life cycle, we started by synthesizing the steps described by existing data life cycle models. To that end, based on the literature review presented in Section II, we selected those with a connecting link to personal data management. We therefore included the abstract data lifecycle model Möller (2013) suggested, as it synthesizes and generalizes several other existing models. The model Alshammari and Simpson (2018) proposed is included as well, since it is derived from Möller (2013), and is the only one that specifically focuses on personal data. Because personal data manifests itself in the consumer/customer data domains in organizations, we also included data life cycle models related to master data management (DAMA International 2009; Levitin and Redman 1993).

Most models, except for Levitin and Redman (1993), start with a planning phase, prior to data acquisition. It serves various purposes – for Möller (2013), it defines the intent for creating the data and the internal requirements, such as data ownership, that will apply to the data post-collection. Alshammari and Simpson (2018) phrase this intent in terms of the planned use of the data, referring to the purpose of data processing, while DAMA International (2009) frames it as a preparatory phase to ensure proper alignment with an organization's system design processes.

All models then describe the step of collecting data and bringing it into an organization's system, which is referred to as creation, collection, obtaining values, acquisition, or publication. By mentioning the CRUD set of operations, Möller (2013) suggests that these steps might be broken down further, in which case a first step would consist of acquiring and collecting the data. A second step would be translating it into an organization's data structure and making it consistently available in its systems. Although not explicitly stated, a similar inference can be drawn from Alshammari and Simpson (2018), who mention a conceptual modeling step at the very beginning, prior to the planning phase, in order to specify the required data, the purposes for which personal data is to be processed, and the logical and physical data models.

The next step revolves around the usage of data and accompanying activities. Here, Möller (2013) leans towards knowledge management/sharing and introduces steps closely related to getting feedback from internal as well as external users, while (Levitin and Redman 1993) emphasizes quality control and generating related results. At this stage, Alshammari and Simpson (2018) distinguish access and usage, but also outline privacy-related steps, such as retention and review/disclosure. DAMA International (2009) centers on data maintenance.

All models also address the end-of-life of data, and comprise a step that corresponds to their removal from processing systems. In that same phase, before removal, Möller (2013) and DAMA International (2009) introduce an archiving step during which data can still be retrieved, while Levitin and Redman (1993) focus on evaluation activities prior to removal.

	Steps		
	Onboarding	***Usage***	***End-of-life***
(1)	Ontology development, planning, creation	Publication, refinement, access, external use, feedback	Archiving, termination
(2)	Define view, implement view, obtain values, update records	Define subview, retrieve, manipulate, present results, use, assessment, analysis, adjust, update records	Obtain values, assessment, analysis, discard
(3)	Plan, specify, enable, create and acquire	Maintain and use	Archive and retrieve, purge
(4)	Conceptual modeling, initiation, collection	Retention, access, usage, review, disclosure	Destruction

Table 1: Data life cycle stages and steps (where 1 = Möller 2013, 2 = Levitin and Redman 1993, 3 = DAMA International 2009 and 4 = Alshammari and Simpson 2018).

As synthesis, and in order to clearly structure the remainder of this study, we can derive three main stages showing through the aforementioned data

life cycle models: onboarding (comprising the planning and collection/creation of data), usage (comprising all steps to be performed as data is stored and processed in systems), and end-of-life (comprising archival and deletion). Tab. 1 presents a summary of data life cycle steps as they appear in the models, classified according to these three stages.

4.2 Data-centric legal requirements

As per our research process, we started by investigating requirements from the GDPR to analyze how data protection regulations impact the data life cycle. We formulated the assumption that principles underpinning these requirements are representative of data protection to a broader extent and would apply to other data protection regulations. We verified this assumption by integrating the CCPA in our analysis in a second step.

In analyzing the GDPR, we excluded the first chapter, which contains definitions and defines the material and territorial scopes of application. Chapters II and III, which contain principles and data rights, were included, as well as the first section of Chapter IV, which indicates data processing organizations' duties. The following sections of Chapter IV were excluded, as they cover security aspects (which we purposefully excluded from our study) and organizational aspects (such as impact assessments, data protection officers, codes of conduct, and certifications). The remaining chapters were not considered, as they deal with legal and judicial aspects that have no impact on data management activities.

With the selected chapters, further legal dispositions were set aside. Art. 10 targets information processing related to criminal convictions, which is a specific case that only applies to legal authorities. Similarly, Art. 23 gives national authorities a possibility to enact stricter rules regarding specific processing cases, such as homeland security, defense, and enhanced protection of individuals, which are also prerogatives of legal authorities. Art. 11 relates to the scope of the GDPR in that it confirms that the processing of data that does not require the identification of individuals falls outside the scope of the regulation. Art. 12 defines modalities according to which organizations are expected to interact with individual requests, for example in terms of responsiveness and clarity, and states that the communication of information regarding data processing should occur without financial retribution. Finally, Art. 31 simply states that organizations must collaborate with supervisory authorities upon request.

To assess the impact of the data protection regulations on data management practices along the data life cycle, we have synthesized the relevant requirements into six categories of rights, and two categories of accountability requirements. These findings are consistent with the analysis provided in the legal literature, regarding rights (Bensoussan et al. 2018, pp. 30–31, Voigt and Von Dem Bussche 2017, pp. 31–38) as well as accountability principles (Nicolaidou and Georgiades 2017, Bensoussan et al. 2018, p. 12, Voigt and Von Dem Bussche 2017, p. 44). Tab. 2 provides an overview of the coverage of each category in the GDPR and the CCPA, and outlines the impacted data life cycle stage, according to the main stages derived in the previous section. We will present these categories in the following paragraphs and map the CCPA 's requirements to each of them.

Requirement	GDPR	CCPA	O	U	E
R: Information	Art. 7, 13, 14	§1798.100	X	X	
R: Access	Art. 15, 18, 20	§1798.110 §1798.115		X	
R: Deletion	Art. 15, 17	§1798.105			X
R: Rectification	Art. 7, 16, 21	N/A		X	
R: Restriction	Art. 18	N/A		X	
R: Consent	Art. 7, 8, 22	§1798.120	X	X	
A: Documentation	Art. 19, 24-30	§1798.130		X	X
A: Authorization	Art. 5, 6, 9	§1798.130		X	

Table 2: Regulatory requirements throughout the data life cycle (where R = right, A = accountability requirement, O = onboarding, U = usage and E = end-of-life).

Right of information. These rights are related to the principle of transparency (European Data Protection Board 2018b), and require that data processing measures be clearly communicated (Nicolaidou and Georgiades 2017, Bensoussan

et al. 2018, p. 17). Concretely, organizations must inform individuals about the data elements they collect and detail the purposes for which they will be used in a clearly identifiable and understandable manner. This applies at the time of data collection, as well as during the entire personal data life cycle (as long as the organization processes related data elements). In these latter cases, information rights are complemented by access rights. These rights are expressed in a similar manner in both the GDPR and the CCPA.

Right of access. As mentioned in the previous paragraph, access rights are similar to those of information, but relate to the disclosure of information during the data use stage only. In that sense, individuals may request to access their data at any time, and organizations must communicate the related data records.

Right of rectification. In the GDPR, a right of rectification complements the right of access (Bensoussan et al. 2018, p. 31), and enables individuals to request that organizations update the data related to them. While the right of access is also present in the CCPA, the right of rectification is not stated in the regulation.

Right of restriction. In the GDPR, a right of rectification enables individuals to contest the processing of the data related to them by an organization (e. g., due to inaccurate data or unauthorized processing). Art. 19 GDPR states that they can request that organizations stop processing the related data until the dispute is resolved. In this case, organizations must effectively "freeze" the processing of data related to the individual. Art. 19 GDPR also states that potential third-party recipients of the related data must be informed of the restriction.

Right of consent. In the GDPR, consent is a foundational principle (Bensoussan et al. 2018; European Data Protection Board 2018a; Voigt and Von Dem Bussche 2017) that requires organizations to collect explicit authorizations from individuals as opt-in. It applies when processing is not based on other available processing bases (such as contract, legitimate interest, or legal obligation), and goes beyond their scope. It should also be collected in case data about children is collected (Art. 8), and when automated decisions will be made based on the collected data (Art. 22). In the CCPA, the right of consent is also present, albeit with a restricted scope – the regulation only enables individuals to opt out of selling their personal data (§1798.120). The right of consent applies in conjunction with the rights of information (at the point of data collection) and of access (during the usage stage).

Right of deletion. Both regulations provide individuals with a right to request that organizations delete personal data that relates to them. This right is not absolute, in the sense that organizations may need to keep said data, or at least parts of it, for other purposes. In the GDPR, these purposes are clearly laid out and refer to the authorization accountability requirements (see below). For instance, organizations may be required to retain personal data in order to comply with other regulations. Once the deletion has occurred, third-party recipients of the related data must also be notified (Art. 19 GDPR). In its §1798.105, CCPA enumerates the situations in which organizations are authorized to retain personal data.

Authorization (accountability requirement). In the GDPR, any type of data processing must satisfy one (or several) of the bases for processing specified in Art. 5, referring to explicit consent (which is required for all automated decision-making), contract execution, compliance with another regulation, safeguarding the individual's vital interests, performance of public interest tasks/exercise of official authority, and legitimate interests. The CCPA does not provide a specific list of processing bases, but §1798.105 nevertheless lists cases in which organizations are allowed to continue data processing, even if deletion has been requested. These cases are similar to the GDPR 's list of processing bases, with an emphasis on fraud prevention and scientific research (which could be construed as legitimate interests), as well as enforcing free speech and other legal requirements.

Documentation (accountability requirement). The documentation requirement appears in both regulations. It stipulates that organizations must

be able to demonstrate the lawfulness of their processing activities (authorization), as well as the fulfillment of the abovementioned rights (Nicolaidou and Georgiades 2017, Voigt and Von Dem Bussche 2017, p. 44). This is necessary, for instance, to enforce the right of access: organizations must have defined and recorded the base(s) and purpose(s) of processing in order to communicate them upon individual request. From a broader perspective, and in case of official inquiry, organizations must be able to demonstrate that they process data according to legal requirements, meaning that they systematically collect the necessary data to ensure proper enforcement.

5 Reference personal data life cycle model for data protection

In this section, we reconcile the data life cycle steps with the data-centric regulatory requirements that we have isolated. We start by introducing a data model for data protection and structural business rules, which concretize the accountability requirements outlined in Section 4.2. Then we introduce a process model to articulate the relationship between data life cycle steps and data rights, organized around three subviews corresponding to the life cycle stages previously identified (onboarding, usage, and end-of-life).

Taken together, the data model, the process model and the business rules form the overarching reference personal data life cycle model for data protection, which we introduce in the following sections.

The data life cycle model has been designed using a semi-formal notation approach, based on the Business Process Modeling Notation (BPMN). We argue that the data life cycle can be expressed as a process, with different steps that create, read, update, and delete data objects, in accordance with the CRUD set of data operations. We chose BPMN due to its popularity for process modeling in both academia and practice. It was also suggested by participants of Focus group 2, so as to make the model approachable.

Both models are complemented by business rules expressed using the semantics of business vocabulary and business rules (SBVR) specification, a standard from the Open Management Group (OMG). It has been designed specifically to formalize compliance rules, and SBVR rules are adequate to support and complement BPMN process models (Cheng et al. 2011; Kluza and Honkisz 2016; Mickeviciute et al. 2017; Skersys et al. 2012a,b). In our case, they ensure that legal requirements are met, and support the alignment of the life cycle process with data management.

5.1 Data model for data protection

In Section 4.2, we established that data protection regulations express accountability requirements, according to which organizations must be in a position to demonstrate compliance with data protection regulations by making sure all personal data processing is authorized and documented. In order to reach this objective, we argue that organizations must define, collect, and maintain personal data objects and attributes, as described by our proposed data model for data protection (Fig. 2).

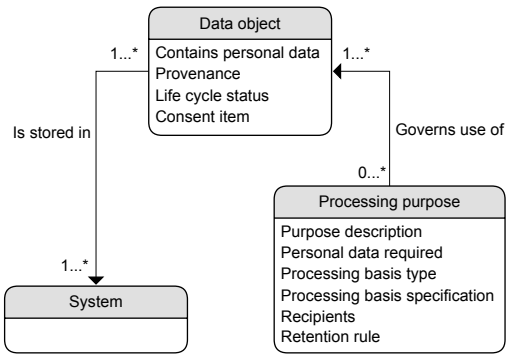

Figure 2: Personal data model for data protection

First, organizations must document the various purposes for which they process personal data, hence we suggest a first data object: *processing purpose*. Purpose documentation should be built around the information regarding the goal, authorization and type(s) of data required. To this end, we propose the following attributes:

- `Purpose description`: This should contain an explanation of the purpose at hand - to what end is personal data processed. For instance, an e-commerce retailer could outline that they need to collect personal data from their customers in order to process orders.
- `Personal data required`: This should list the personal data components that are required by the purpose, ideally in reference to data objects and/or attributes in the organization's data model. For instance, the e-commerce retailer would require a customer's name, address, birth date and credit card information in order to process orders.
- `Processing basis type`: This should indicate possible processing bases (e. g. a contract according to Art. 5 GDPR) which must be specified to authorize data processing.
- `Processing basis specification`: This should describe the specific basis for the purpose at hand (e. g. details of a specific contract). In case the processing basis is consent, the specification should reflect the yes/no question that individuals will be asked for permission granting.
- `Recipients`: If the purpose entails transmitting data to third-party recipients, they should be specified here, so that organizations can notify such recipients in case restriction or deletion requests occur (Art. 19 GDPR).
- `Retention rule`: If the purpose entails a specific retention rule (e. g. duration for keeping financial documents), it should be specified here.

For the *processing purpose* data object, all attributes must be recorded, except the `retention rule`, as it is not mandatory to specify ending conditions for processing activities. Consequently, the following structural business rules apply to the *processing purpose* data object:

- It is necessary that *processing purpose* has `purpose description` and `personal data required` and `processing basis type` and `processing basis specification`.
- It is possible that *processing purpose* has `recipients`.
- It is possible that *processing purpose* has `retention rule`.
- It is necessary that *processing purpose* refers to *personal data object*.

When it comes to information recorded inside data objects, we suggest adding the following attributes to existing *data objects*:

- `Contains personal data`: This should be a Boolean value specifying whether a data object contains personal data.
- `Provenance`: This should specify whether a data object has been directly collected from the data subject themselves, or whether it was transmitted by a third-party. Organizations may also choose to introduce a more fine-grained classification. This would, for instance, enable organizations to clarify their data selling duties as per §1798.115d CCPA, which states that they cannot resell data that was itself sold to them without the data subject's agreement.
- `Consent item`: This should be a Boolean value, specifying whether an individual has opted in or out regarding consent-based processing purposes.
- `Life cycle status`: This should specify whether a data object is available for regular use or whether it has been marked for archival (e. g. in the case of a deletion request occurring while a processing purpose's retention rule is still ongoing) or restriction (in the case of a restriction request).

Consequently, the following business rules apply to the *data object* data object:

- It is necessary that *data object* has `contains personal data`.
- It is necessary that *data object* has `provenance`.
- It is necessary that *data object* has `life cycle status` if `contains personal data` is `true`.

- It is possible that *data object* has `consent item` if `contains personal data` is `true`.
- It is necessary that *data object* refers to *processing purpose* and *system* if `contains personal data` is `true`.

Finally, we suggest documenting *systems* of storage using a distinct data object. The ability to locate storage instances of data records is crucial for the disclosure and deletion activities and has been cited as a significant difficulty in several of the focus groups we conducted. This aspect is confirmed by Bensoussan et al. (2018, p. 23), highlighting the need for detailed mapping of collected data. Peyret et al. (2017) points in the same direction.

5.2 Data life cycle model for data protection

In this section, we present the reference personal data life cycle model with its detailed subviews, corresponding to each of the data life cycle main stages (onboarding, usage, and end-of-life). Fig. 3 depicts the data life cycle reference model, which comprises 12 steps. For each step, we specify CRUD operations that should be conducted on data objects and/or attributes in order to operationalize the regulatory rights and accountability requirements, as well as related operational business rules.

5.2.1 Subview: Onboarding

The entry point in the data life cycle is a requirement for new personal data (A1) - this step mirrors the planning step, as expressed in the models we analyzed in Section 4.1. It is related to the right of information, as organizations must define and expose in advance the bases and purposes of processing related to the personal data they intend to collect. In the first step, organizations must define in advance the bases and purposes of processing for personal data, which is a key departure from previous data life cycle models. At this stage, the data in *processing purpose* is `created`.

The next three steps reflect activities necessary to bring data into an organization's system and synthesize those described by the models we reviewed in the previous section. *Communicate processing modalities* and *collect data components* correspond to the data collection. *Record data object* corresponds to the moving of data into an organization's database/data model.

In the second step (A2), the processing basis and purposes should be displayed when collecting data from individuals (e. g. on a website). For that purpose, the data in *processing purpose* is `read`, and the following business rule applies, concretizing informational duties:

- *R1*: It is obligatory that *processing purpose* is disclosed.

In the third step (A3), data components are collected from the individual. It specifies which specific data components should be collected according to the processing purpose. The data in *processing purpose* is therefore `read`, and the following business rule apply:

- *R2*: It is obligatory that `personal data required` is collected.
- *R3*: It is obligatory that `consent item` is collected if `processing basis type` is `consent`.

In the fourth step (A4), data components are translated into the organization's structured data model. At this stage, the data in *data object* is `created` in the system.

5.2.2 Subview: Usage

After data is created, it must be deployed in the appropriate systems. *Deploy data* (B1) is derived from the publication step Möller (2013) suggested, in the sense of making data available for usage. Participant feedback from focus groups indicated that organizations often operate with highly distributed system landscapes and need to deploy the data in several other systems that require it. For instance, in a multinational organization, data created in one ERP system may need to be deployed in other ERP systems (e. g. region-specific). Another example is data transfer in data lakes or other advanced analytics systems, separate from

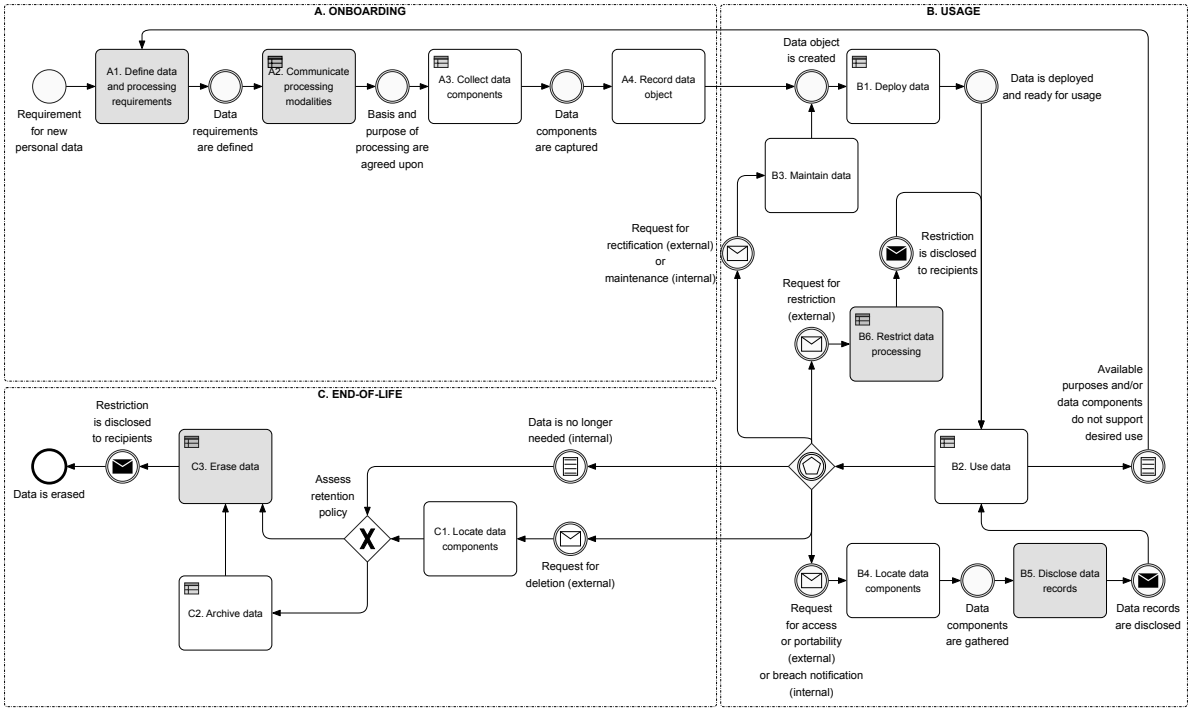

Figure 3: Reference personal data life cycle model for data protection. Steps highlighted in grey mirror data protection requirements and are additions to traditional data life cycle models.

traditional enterprise systems. Therefore, recording target systems at the step of deployment could ease the creation of a system map for personal data processing, as Bensoussan et al. (2018, p. 23) recommended. To that effect, at this step (B1), the data in *system* is read and the *data object* is updated. Additionally, the following business rule applies:

- *R4*: It is obligatory that deployment *system* is referred to in *data object*.

Next, *use data* (B2) reflects the *processing purposes*, and was included in all analyzed models. At this stage, *processing purpose* and *data object* are `read`, and the following business rules applies:

- *R5*: It is obligatory that usage of *data object* conforms to *processing purpose*.

If the desired purpose cannot be fulfilled using available data objects and purposes, the life cycle process starts again at Step A1, as data and processing requirements need to be reviewed and extended, leading to a new instance of processing purpose. Following this, the new purpose must be communicated and/or additional data must be collected accordingly.

Contrary to Alshammari and Simpson (2018), we did not include a retention step, and argue that retention is better described in terms of the `retention rule` attribute (defined in Section 5.1) than as a distinct step. The disclosure step Alshammari and Simpson (2018) suggested represents the exchange of personal data between different organizations. We did not include a similar step in our model. From a regulatory standpoint, both the GDPR and the CCPA stipulate that data exchanges must be announced as distinct processing purposes and are therefore encapsulated in the use data (B2) step.

Alshammari and Simpson (2018) suggest two steps for data communications - review and disclosure. Their review step originates from individuals

	Create	Read	Update	Delete
A1. Define data and processing requirements	Processing purpose *(R1)*			
A2. Communicate processing modalities		Processing purpose		
A3. Collect data components		Processing purpose *(R2, R3)*		
A4. Record data object	Data object			
B1. Deploy data		System *(R4)*	Data object *(R4)*	
B2. Use data		Data object, Processing purpose *(R5)*		
B3. Maintain data		Processing purpose	Data object	
B4. Locate data components		Data object System		
B5. Disclose data records		Data object Processing purpose		
B6. Restrict data processing		Processing purpose *(R6)*	Data object *(R6)*	
C1. Locate data components		Data object System		
C2. Archive data		Processing purpose *(R7)*	Data object *(R7)*	
C3. Erase data		Processing purpose *(R8)*		Data object *(R8)*

Table 3: Overview of CRUD operations applied to data object at each data life cycle step (related business rule mentioned when applicable).

and corresponds to the rights of access and rectification, which we have chosen to model as two distinct steps, namely *disclose data records* and *maintain data*. This articulation reflects the two rights individually, and that a disclosure does not necessarily prompt subsequent action from an individual. We also argue that a change in the data does not always originate from an individual request and can be triggered internally, for instance as part of data quality checks or routine data maintenance.

When maintaining data (B3), the data in *processing purpose* and *data object* is `updated`. At this point, relationships with certain instances of processing purpose may be removed (following a right of restriction request) or added (following authorization of further processing).

Following a right of access request, data must be located (B4) - for that purpose, the data in *data object* and system is `read`. In order to disclose data to individuals (B5), the data in *data object* and *processing purpose* is `read` and formatted for communication. Disclosure can also occur following a data breach. In this case, it is triggered internally when the breach is discovered, and the organization must communicate a list of compromised *data objects* (B4) to individuals (B5).

In the context of this study, we treat the right of portability as a variant of data disclosure, as it is also about communicating data records, with the added requirement of doing so in a standard, machine-readable format.

Following a right to restriction request under the GDPR, organizations must stop processing the related data until further notice (B6) and inform third-party recipients of the restriction. At this point, *data object* and *processing purpose* are `updated`. We also suggest that organizations document a "restriction" processing purpose to effectively freeze data processing with the following business rule:

- *R6*: It is obligatory that `life cycle status` of *data object* is updated if *processing purpose* of *data object* is "restriction".

5.2.3 Subview: End-of-life

The end-of-life stage is triggered by a deletion request from the individual or by the ending of a predefined `retention rule`. Here again, related data objects must be located in the organization's system landscape (C1) before they can be archived or deleted. At this point, the data in *data object* and *system* is `read`.

As previously mentioned, when faced with a deletion request, it should be determined whether data can be erased, or whether it should be kept.

This retention aspect has been cited as a significant difficulty during Focus groups 1 and 2, and participants mentioned that retention checks were not automated in their organizations.

Depending on the outcome of the retention check based on the `retention period` attribute, the related data elements would either be archived (C2) or removed (C3).

In the case of archival (C2), data in *processing purpose* is `read` and *data object* is `updated` (specifically, the `life cycle status` attribute). In addition, the following business rule applies:

- *R7*: It is obligatory that `life cycle status` of *data object* is changed if `retention rule` of *processing purpose* is valid.

In the case of erasure (C3), data in *processing purpose* is `read` and *data object* is `deleted`. In addition, the following business rule applies:

- *R8*: It is obligatory that *data object* is erased if `retention rule` of *processing purpose* is void.

By erasure, we mean both deletion and anonymization. As data is anonymized, meaning that all personally identifiable information is deleted, it no longer falls under the scope of data protection regulations, and thus exits the personal data life cycle.

Tab. 3 provides a condensed overview of CRUD operations carried-out throughout life cycle step.

6 Summary and discussion

The purpose of this study was to analyze the impact of data protection regulations from a data management perspective. To that end, we have investigated two distinct aspects of such regulations to develop of reference personal data life cycle model for data protection, which constitutes our main contribution.

First and foremost, data protection regulations grant a set of rights to individuals, designed to foster transparency about data processing, and clearly set the scope of data processing activities. The enablement of these rights translates into requirements for organizations, which we have represented using the concepts of life cycle process and business rules, in order to show how these requirements affect data management practices. This objective mirrors our first research question (RQ 1).

In addition to enabling data protection rights, organizations must be in a position to demonstrate that their processing of personal data has been lawful and authorized, and that it occurs within the contours of the regulatory rights and requirements. This obligation reflects the new principle of accountability, according to which organizations must document the compliance of their processing activities. To that effect, we have proposed a set of data objects and attributes that should be recorded along the steps of the data life cycle in order to provide a basis for such documentation. Furthermore, our model shows that such documentation (especially as it relates to processing purposes) should begin before any data is collected. In that sense, it matches the requirements for privacy by design and by default, particularly as formulated in the GDPR, which states that measures should be implemented "both at the time of the determination of the means for processing and at the time of the processing itself" (Art. 25). This mirrors our second research question (RQ 2).

This study contributes to both research and practice. For research, it complements existing studies on the data life cycle by elaborating on the under-researched domain of personal data and by bringing in a regulatory perspective. By suggesting a semi-formal notation, we translate the emerging regulatory requirements into a set of rules. It also links up with related studies from the business process management domain. For instance, Agostinelli et al. (2019) also use BPMN to model processes triggered by the exercise of individual rights (e. g. access, rectification), aiming to tackle them from process management perspective, which our study supplements by outlining data-related requirements to support compliance processes. Practitioners may benefit from the standardized notation of data protection issues to better understand data protection requirements,

and identify potential blind spots in their operations.

7 Limitations and future research outlook

In this study, we purposefully bound our analysis of data protection regulations to the concept of the data life cycle. This informs organizations about critical steps that need to be addressed to tackle data protection requirements along the main stages of the data life cycle (onboarding, usage, end-of-life).

However, we only consider usage from the data provisioning perspective and did not analyze the actual data usage in detail. We argue that usage would be better described using concepts other than the data life cycle, such as data lineage, data flows or information supply chains. Such concepts would help analyze the information products and subsequent insights that can be derived from personal data, which would be useful, for instance, in the context of data protection impact assessments of data analytics activities. Similarly, we limited the suggested data attributes to the ones that strictly relate to legal requirements on an abstract level. A formal data model enriched with business rules could be developed for typical personal data objects, incorporating our suggested attributes. A classification of typical usage patterns could also be described in order to enhance the mapping of the retention policy to groups of data objects. Organizations would benefit from further describing the way data is used, for example in terms of roles, access control and permissions, and processes. In that regard, future research should make the link with responsibility definitions from the data governance domain, as well as with the abundant business process management literature stemming from the regulatory compliance management domain.

References

Agostinelli S., Maggi F. M., Marrella A., Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. In: Information Systems Engineering in Responsible Information Systems. Lecture Notes in Business Information Processing Vol. 350. Springer, pp. 10–22

Alshammari M., Simpson A. (2018) Personal Data Management: An Abstract Personal Data Lifecycle Model. In: Business Process Management Workshops. Lecture Notes in Business Information Processing Vol. 308. Springer, pp. 685–697

Bélanger F., Crossler R. E. (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. In: MIS Quarterly 35(4), pp. 1017–1042

Bensoussan A., Avignon C., Bensoussan-Brulé V., Forster F., Torres C. (2018) Règlement Européen sur la Protection des Données: Textes, Commentaires et Orientations Pratiques. Bruylant

Burt A. (2019) Privacy and Cybersecurity Are Converging. Here's Why That Matters for People and for Companies. In: Harvard Business Review 10, pp. 1–6

California State Senate (2018) California Consumer Privacy Act. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cheng R., Sadiq S., Indulska M. (2011) Framework for Business Process and Rule Integration: A Case of BPMN and SBVR. In: Business Information Systems. Lecture Notes in Business Information Processing Vol. 87. Springer, pp. 13–24

Collins English Dictionary (2019) Life cycle definition and meaning. Dictionary Entry

Commission Nationale de l'Informatique et des Libertés (2018) RGPD : passer à l'action. https://www.cnil.fr/fr/rgpd-passer-a-laction

DAMA International (2009) The DAMA Guide to the Data Management Body of Knowledge. Technics Publications

De Hert P., Papakonstantinou V. (2012) The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals. In: Computer Law & Security Review 28(2), pp. 130–142

De Hert P., Papakonstantinou V. (2016) The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals? In: Computer Law & Security Review 32(2), pp. 179–194

Debet A., Massot J., Métallinos N. (2015) Informatique et libertés: la protection des données à caractère personnel en droit français et européen. Les intégrales 10. Lextenso

European Data Protection Board (2018a) Guidelines On Consent Under Regulation 2016/679 (WP259, rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

European Data Protection Board (2018b) Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

European Parliament and Council of the European Union (2016) Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Greenberg J. (2003) Metadata Generation: Processes, People and Tools. In: Bulletin of the American Society for Information Science and Technology 29(2), pp. 16–19

Guadamuz A. (2017) Developing a Right to be Forgotten. In: EU Internet Law: Regulation and Enforcement. Springer, pp. 59–76

Hakim S., Li Z., Pan Y., Zaunseil F., Chi H., Zhou W. (2018) The Impact of General Data Protection Regulation (GDPR) on Data Management Platforms (DMP): A Policy Perspective. In: Management & Data Science 2(3)

Hevner A. R., March S. T., Park J., Ram S. (2004) Design Science in Information Systems Research. In: MIS Quarterly 28(1), pp. 75–105

Higgins S. (2008) The DCC Curation Lifecycle Model. In: International Journal of Digital Curation 3(1), pp. 134–140

Hirschheim R., Klein H. K. (2012) A Glorious and Not-So-Short History of the Information Systems Field. In: Journal of the Association for Information Systems 13(4), pp. 188–235

Kluza K., Honkisz K. (2016) From SBVR to BPMN and DMN Models. Proposal of Translation from Rules to Process and Decision Models. In: Artificial Intelligence and Soft Computing. Lecture Notes in Computer Science Vol. 9693. Springer, pp. 453–462

Levitin A. V., Redman T. C. (1993) A model of the data (life) cycles with application to quality. In: Information and Software Technology 35(4), pp. 217–223

McKeever S. (2003) Understanding Web content management systems: evolution, lifecycle and market. In: Industrial Management & Data Systems 103(9), pp. 686–692

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

Métille S., Raedler D. (2017) Swiss Data Protection Act reform set in motion. In: Data Protection Leader 14(2), pp. 14–16

Mickeviciute E., Butleris R., Gudas S., Karciauskas E. (2017) Transforming BPMN 2.0 Business Process Model into SBVR Business Vocabulary and Rules. In: Information Technology And Control 46(3), pp. 360–371

Mitrou L. (2017) The General Data Protection Regulation: A Law for the Digital Age? In: EU Internet Law: Regulation and Enforcement. Springer, pp. 19–57

Modritscher F. (2009) Semantic Lifecycles: Modelling, Application, Authoring, Mining, and Evaluation of Meaningful Data. In: International Journal of Knowledge and Web Intelligence 1(1/2), pp. 110–124

Möller K. (2013) Lifecycle Models of Data-centric Systems and Domains: The Abstract Data Lifecycle Model. In: Semantic Web 4(1), pp. 67–88

Nicolaidou I. L., Georgiades C. (2017) The GDPR: New Horizons. In: EU Internet Law: Regulation and Enforcement. Springer, pp. 3–18

Ofner M., Otto B., Oesterle H., Straub K. (2013) Management of the master data lifecycle: a framework for analysis. In: Journal of Enterprise Information Management 26(4), pp. 472–491

Palanisamy M., Nandle R. (2018) Understanding India's draft data protection bill. https://iapp.org/news/a/understanding-indias-draft-data-protection-bill/

Parliament of the Republic of India (2018) The Personal Data Protection Bill. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Payne A., Frow P. (2005) A Strategic Framework for Customer Relationship Management. In: Journal of Marketing 69(4), pp. 167–176

Peffers K., Tuunanen T., Rothenberger M. A., Chatterjee S. (2007) A Design Science Research Methodology for Information Systems Research. In: Journal of Management Information Systems 24(3), pp. 45–77

Peyret H., Cullen A., McKinnon C., Blissent J., Iannopollo E., Kramer A., Lynch D. (2017) Enhance your Data Governance to Meet New Privacy Mandates. Forrester Research. https://www.forrester.com/report/Enhance+Your+Data+Governance+To+Meet+New+Privacy+Mandates/-/E-RES135462

Prat N., Comyn-Wattiau I., Akoka J. (2015) A Taxonomy of Evaluation Methods for Information Systems Artifacts. In: Journal of Management Information Systems 32(3), pp. 229–267

Rubio M. (2019) A bill to impose privacy requirements on providers of internet services similar to the requirements imposed on Federal agencies under the Privacy Act of 1974. https://www.govinfo.gov/app/details/HOB-2019/HOB-2019-s142/summary

Saarijärvi H., Karjaluoto H., Kuusela H. (2015) Customer Relationship Management: The Evolving Role of Customer Data. In: Marketing Dynamism & Sustainability: Things Change, Things Stay the Same. Developments in Marketing Science: Proceedings of the Academy of Marketing Science. Springer, pp. 505–515

Sinaeepourfard A., Garcia J., Masip-Bruin X., Mar (2016a) A comprehensive scenario agnostic Data LifeCycle model for an efficient data complexity management. In: 2016 IEEE 12th International Conference on e-Science (e-Science). IEEE, pp. 276–281

Sinaeepourfard A., Masip-Bruin X., Garcia J., Mar (2016b) A survey on data lifecycle models: discussions toward the 6Vs challenges.. UPC BarcelonaTech. https://www.ac.upc.edu/app/research-reports/html/RR/2015/18.pdf

Skersys T., Tutkute L., Butleris R. (2012a) The enrichment of BPMN business process model with SBVR business vocabulary and rules. In: Proceedings of the 34th International Conference on Information Technology Interfaces. IEEE, pp. 65–72

Skersys T., Tutkute L., Butleris R., Butkiene R. (2012b) Extending BPMN Business Process Model with SBVR Business Vocabulary and Rules. In: Information Technology And Control 41(4), pp. 356–367

Staab S., Studer R., Schnurr H., Sure Y. (2001) Knowledge processes and ontologies. In: IEEE Intelligent Systems 16(1), pp. 26–34

Tapsell J., Akram R. N., Markantonakis K. (2018) Consumer Centric Data Control, Tracking and Transparency – A Position Paper. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/

12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, pp. 1380–1385

Tikkinen-Piri C., Rohunen A., Markkula J. (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies. In: Computer Law & Security Review 34(1), pp. 134–153

Voigt P., Von Dem Bussche A. (2017) The EU general data protection regulation (GDPR): A Practical Guide. Springer

Warren S., Brandeis L. (1890) The Right to Privacy. In: Harvard Law Review, pp. 193–220