Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Enhancing Information Governance with Enterprise Architecture Management: Design Principles Derived from Benefits and Barriers in the GDPR Implementation

Fabian Burmeister
University of Hamburg
burmeister@informatik.uni-hamburg.de

Dominik Huth
Technical University of Munich
dominik.huth@tum.de

Paul Drews
Leuphana University of Lüneburg
paul.drews@leuphana.de

Ingrid Schirmer
University of Hamburg
schirmer@informatik.uni-hamburg.de

Florian Matthes
Technical University of Munich
matthes@tum.de

Abstract

Businesses today are increasingly dependent on how they transform information into economic value, while simultaneously being compliant with intensified privacy requirements, resulting from legal acts like the General Data Protection Regulation (GDPR). As a consequence, realizing information governance has become a topic more important than ever to balance the beneficial use and protection of information. This paper argues that enterprise architecture management (EAM) can be a key to GDPR implementation as one important domain of information governance by providing transparency on information integration throughout an organization. Based on 24 interviews with 29 enterprise architects, we identified a multiplicity of benefits and barriers within the interplay of EAM and GDPR implementation and derived seven design principles that should foster EAM to enhance information governance.

1. Introduction

Businesses today are increasingly dependent on how they perform big data analytics initiatives to transform personal data into valuable information. The ability to distill key insights from personal data has evolved into a major source of competitive advantage [1, 2]. According to the World Economic Forum, personal data represents a majority in big data aggregations and has become a new asset class providing the oil of the 21st century [3]. In fact, recent statistics predict that big data analytics' global revenue will increase by 63.1% from $168 billion in 2018 to $274 billion in 2022 [4]. Simultaneously, the rapidly growing volume, velocity and variety of the data deluge are accompanied by numerous information risks, colossal data leaks and the need for greater compliance with legal privacy demands imposed by multinational laws, such as the General Data Protection Regulation (GDPR) [1, 5, 6]. Consequently, realizing sophisticated information governance that balances the beneficial use and protection of information, including accumulations of personal data, has become a critical issue for senior business and IT management [1, 2, 7]. The literature defines information governance as "a holistic approach to manage and use information for business benefits that encompasses information quality, information life cycle management, and security, privacy and compliance" [8]. Scholars state that information governance complements IT governance by focusing on the information artifact rather than the physical IT artifact [1, 2]. Thereby, the "inadequacy of IT governance to deal with the decisive role of information in present-day organizations" [9] is compensated. In this regard, this paper follows Tallon et al.'s definition of IT artifacts being bundles of properties packaged in hardware or software and information artifacts being logical sets of data [1]. However, while IT governance has been a focus in information systems research (ISR) for more than two decades, research on information governance is still in its infancy [2, 9, 10].

A key instrument for supporting IT governance in its main task of business IT alignment is the enterprise architecture management (EAM) [11], which is defined as a means to plan, coordinate, and guide the continuous digital transformation in organizations by fostering the use of a common language and providing a consistent decision base [12]. By providing transparency through as-is and to-be models of business and IT artifacts and their relations in the enterprise architecture (EA), EAM supports strategic decision-making of IT executives [11, 12]. As IT governance and information governance can be seen as coequal subsets of corporate governance [13], it is implicated that EAM can provide a foundation for information governance as well, if capturing how the information artifact is incorporated in an organization.

URI: https://hdl.handle.net/10125/64430
978-0-9981331-3-3

In addition, the GDPR's entry into force in May 2018 has triggered information governance efforts all over the world and obliged enterprises to address the information artifact more intensively in their EAM [6]. As non-compliance with the GDPR can result into penalties up to four percent of an organization's revenue [5, Art. 83], realizing GDPR compliance has become one of the current main issues of information governance [14].

In this paper, we aim to understand and improve the current interplay of EAM and information governance using the example of GDPR implementation. For this purpose, our study follows three research questions:

RQ1: *What are the benefits of EAM for GDPR implementation and vice versa?* As the first objective of our study, we intend to reveal how EAM and GDPR implementation currently benefit from each other.

RQ2: *Which barriers currently exist in supporting GDPR implementation with EAM?* Our second objective refers to the identification of key factors that dampen the success of EAM in supporting GDPR implementation.

RQ3: *Which design principles can be derived from the benefits and barriers of GDPR implementation to foster EAM in enhancing information governance?* Finally, by learning from the benefits and barriers, our third objective is to derive design principles that improve the interplay of EAM and information governance.

To answer these research questions, we conducted expert interviews [15] with 29 enterprise architects in 24 organizations of different industries. The remainder of this paper is organized as follows. In the next section, we summarize related research. Afterwards, we outline our research approach and present our results. Finally, we close the paper with a discussion and conclusion.

2. Related research

In our research context, we identified three streams of related research. The first stream delimits information governance, describes its basics and outlines its logical interrelation with the GDPR. The second stream deals with the fundamentals and challenges of EAM. The third stream refers to earlier research that combines EAM with issues of information governance, especially the GDPR.

2.1. Information governance and the GDPR

According to a survey in 2018, 60% of information managed by organizations has no business, legal or regulatory value [14]. To dispose this information debris, information governance aims to optimize and leverage information use while sustaining security and meeting legal obligations [2]. Therefore, information governance consists of "capabilities or practices for the capture, valuation, storage, usage, control, access, archival, and deletion of information over its life cycle" [1]. Data governance, however, refers to techniques like data cleansing and de-duplication to ensure that the raw data gathered by organizations is accurate, reliable and not redundant [2, 9]. Data governance as such is "the most rudimentary level at which to implement information governance" [2]. IT governance, in comparison, can be defined as "the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" [16]. Thus, IT Governance, seeks to ultimately align business objectives with IT strategy to deliver business value [2]. Essentially, information governance differs in that it focuses on optimizing the value and protection of information, whereas IT governance encompasses all activities relating to IT management with the aim of generating the most benefit out of IT investments [8, 17]. Nevertheless, some similarities can be perceived as well. In line with the three types of practices in IT governance, Weber et al. [18] suggest that information governance consists of decision-maker roles (structural practices), decision tasks (procedural practices) and responsibilities (relational practices). Using the five decision domains of IT governance according to Weill and Ross [19], Khatri and Brown [20] portray a parallelism of data principles (IT principles), data quality (IT architecture), metadata (IT infrastructure), data access (IT applications) and data life cycle (IT investments). Tallon et al. [1] state that the degree of similarity implies a positive extrapolation of factors already known from the realm of governing physical IT artifacts to governing information artifacts.

In a long-term study, 81% of organizations reported progress on their information governance programs in 2018, compared to only 33% in 2010 [14]. Despite these positive signs, a survey directed by Cisco in 2019 shows that only about half of organizations indicated GDPR readiness, even though the GDPR is in force since May 2018 [21]. Burmeister et al. [6] divided the obligations for enterprises caused by the GDPR into four categories: compliance with superior principles (e.g., transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity), information obligations (e.g., data breach notifications and record of processing activities), satisfaction of data subject's rights (e.g., right of access, right of rectification, right to erasure) and organizational and technical measures (e.g., pseudonymization, privacy by design). Current main challenges for enterprises in complying with these obligations are fulfilling access and deletion requests of data subjects, meeting privacy by design and security requirements, and inventorying data [21]. Referring back to the definition of information governance, it is obvious that the GDPR and information governance reinforce each other by shared goals. The GDPR legitimizes information governance that in turn initiates the activities to comply with the GDPR.

2.2. Enterprise architecture management

The term architecture is defined as “the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution” [22]. The EAM documents the EA, where the system is a company or authority, from a holistic perspective, creates views and metrics for its stakeholders and develops the EA to reach strategic goals [12]. For this purpose, EAM refers to EA meta-models that structure the artifacts and relations of EA along layers. Winter and Fischer [23] identified five common layers: business (e.g., strategic goals), process (e.g., business processes, information flows), integration (e.g., interfaces), software (e.g., software components, data structures) and technology (e.g., hardware and network components). EA meta-models seek to provide a template for deriving instances of as-is and to-be EA models that address information needs of stakeholders [6, 12]. Thereby, EAM provides transparency on the complex relations between business and IT artifacts and supports the planning of future scenarios. To maintain and develop the EA based on these models, EAM refers to EA frameworks, such as TOGAF [24], which provide rules and methods to manage the life cycle of EA [12]. As such, “EAM goes beyond EA modeling and includes management tasks of planning and controlling business changes from an architectural perspective” [25].

In their paper from 2013, Hauder et al. [12] surveyed 50 organizations to investigate the major challenges in realizing EAM. Most notably, ad hoc and unclear EA demands hinder the success of EAM departments. In addition, EAM efforts often encounter unclear business objectives. Other top challenges refer to the lack of experienced enterprise architects on the job market, the pressure resulting from the fast changing organizational environment and the perception that EAM is a primarily IT focused function. With our study, we seek to verify the topicality of these challenges and to examine to what extent they hinder GDPR implementation.

2.3. EAM for information governance

In their paper “15 Years of Enterprise Architecting at HICSS: Revisiting the Critical Problems” from 2017, Kaisler and Armour state that “security and privacy are critical and mandatory at many layers of IT architecture and business architecture” and that “there is a need for EAs of the future to allocate more resources to these areas, and that the architects be more creative in developing protective schemes” [26]. However, research that integrates EAM with security, privacy and analytics aspects, not to mention information governance, is still rather scarce [6, 26]. Karjoth et al., for instance, portray IBM’s enterprise privacy architecture as “a methodology that allows enterprises to maximize the business use of personal information while respecting privacy concerns and regulations” [27]. However, although the enterprise privacy architecture contains essential building blocks towards ensuring privacy (privacy regulation analysis, management reference model, privacy agreements framework, technical reference architecture), it provides rather a superficial guideline for organizations and does not illustrate concrete relations to the EA [6, 27]. Other approaches refer to the setup of an enterprise security architecture, which seeks to align information security controls with business objectives [28]. Shariati et al. [28] reviewed five approaches towards an enterprise security architecture and summarized that business and IT artifacts are often developed isolated from security artifacts, why more research on an integration of security aspects into the EA is needed. To address this demand, Burmeister et al. [6] derived a privacy-driven EA meta-model that proposes an additional security layer next to the other layers of EA. They argue that EA models can be a key to GDPR compliance when capturing privacy- and security-related aspects. For example, modeling applications that process personal data supports the record of processing activities, required by the GDPR [5, Art. 30]. However, the authors clarify neither how organizations can implement this meta-model nor what specific benefits and barriers organizations encounter when using EAM for GDPR implementation.

To conclude, research on the interplay of EAM and information governance is still at an early stage, even though researchers explicitly underline this need [26]. While there are some architectural models that intend to provide first steps to address this research gap [6, 27, 28], there is a great lack of understanding the specific benefits and barriers of EAM in the context of GDPR implementation. Moreover, concrete guidelines in form of design principles that organizations should follow to closer align EAM with big data analytics and privacy departments have to be identified by empirical insights. By following our research questions, we seek to address this research gap and to support organizations in moving EAM forward to enhancing information governance.

3. Research approach

Design principles capture knowledge about instances of a class of artifacts in ISR, which is helpful for both technology and management oriented audiences [29]. According to Hevner and Chatterjee, “a principle can also be formed as a rule or a standard of conduct” [30]. In Gregor’s taxonomy of theory types in ISR, design principles fall into the theory for design and action, which focuses on “explicit prescriptions (e.g., methods, techniques, principles of form and function)” [31]. In EAM research, design principles have been developed in different contexts [32, 33, 34]. However, Stelzer [32] criticizes that design principles for EAM are often derived from case studies on single enterprises and are not generic. In addition, they often refer to constraints of the EA, but do not describe how the EAM itself has to be conducted. To address this lack, we conducted a cross-industry study and followed a design science oriented research approach [35], which is common for proposing design principles [33]. Figure 1 illustrates the four consecutive steps of our research:

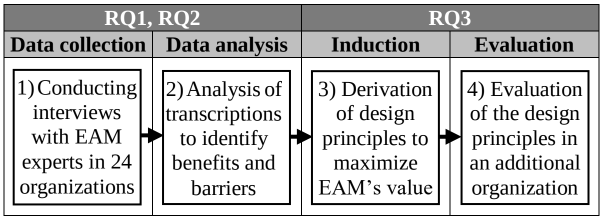
RQ1, RQ2
RQ3
Data collection
Data analysis
Induction
Evaluation
1) Conducting interviews with EAM experts in 24 organizations
2) Analysis of transcriptions to identify benefits and barriers
3) Derivation of design principles to maximize EAM's value
4) Evaluation of the design principles in an additional organization

Figure 1. Research approach

3.1. Data collection

During the first step, we conducted qualitative expert interviews according to Myers and Newman [15] in 24 internationally active organizations based in German-speaking countries. The interviews allowed us to access the thoughts of the 29 participants, mainly enterprise architects, on the current interplay of EAM and GDPR implementation. While we selected the organizations based on the diversity of industries, varied sizes, diverse business models and amount of personal data they are processing, we selected the interviewees based on their long experience in EAM. The heterogeneity allowed us to improve the sample and the generalizability of the results by covering a broad spectrum of perspectives and concerns. Table 1 gives an overview of the interviews.

Table 1. Interview details

No.	Industry	Employees	Interviewee role	Duration
I1	Logistics	5,000-15,000	Enterprise architect	72 min.
I2	Insurance	<5,000	Business architect	62 min.
I3	Government	15,001-50,000	Lead IT strategy	61 min.
I4	Automotive	>50,000	Lead enterprise architect	58 min.
I5	Consulting	5,000-15,000	Lead enterprise architect	52 min.
I6	Insurance	5,000-15,000	Enterprise architect	57 min.
I7	Manufacturing	15,001-50,000	Lead enterprise architect	40 min.
I8	Insurance	15,001-50,000	Enterprise architect	43 min.
I9	Logistics	5,000-15,000	Lead enterprise architect	37 min.
I10	Insurance	5,000-15,000	Enterprise architect	48 min.
I11	IT services	<5,000	Enterprise architect	47 min.
I12	Consumables	15,001-50,000	Enterprise architect	65 min.
I13	IT services	15,001-50,000	Lead enterprise architect	45 min.
I14	Banking	15,001-50,000	Enterprise architect (2)	60 min.
I15	Insurance	<5,000	Chief IT architect	57 min.
I16	Automotive	>50,000	Enterprise architect (2)	52 min.
I17	Banking	<5,000	Enterprise architect	40 min.
I18	Logistics	15,001-50,000	Enterprise architect	45 min.
I19	Banking	5,000-15,000	IT architect	53 min.
I20	Sports	<5,000	Lead IT strategy	65 min.
I21	IT services	>50,000	IT solution architect	54 min.
I22	Automotive	>50,000	Enterprise architect	60 min.
I23	Insurance	5,000-15,000	Enterprise architect (4)	62 min.
I24	IT services	<5,000	IT architect	36 min.

We relied on a semi-structured interview guide with open-ended questions to ensure coverage of relevant aspects, while also leaving space for discussing particular interests of the interviewees. Key questions asked and scheduled in the interview guide referred to (1) the use of EAM to maximize information value and to support GDPR compliance, (2) information exchange between EAM, analytics and privacy departments, (3) the tools used by these departments in daily work, (4) the mutual benefits of EAM and GDPR implementation, (5) major barriers in realizing EAM. To inspire the discussion in the interviews, we considered the challenges identified by Hauder et al. [12] and showed exemplary EA meta-models [6, 23, 24]. We conducted two thirds of the interviews by phone, the other third face-to-face. All interviews were recorded and then transcribed and coded using MAXQDA (version 18). In total, 1,271 minutes were recorded and the material counted 100,226 words.

3.2. Data analysis

To extract valuable insights from the transcriptions, we conducted a qualitative content analysis on the data material by following the process of inductive category development according to Mayring [36]. We considered Saldaña's [37] advice that multiple coding cycles are necessary to ensure a rigorous analysis, as two coders collaboratively conducted three coding cycles in sum. In the first coding cycle, the induction allowed us to get an overview of the content and to code any aspects of relevance by open coding [36]. As a result, we had 11 initial codes, including 'tasks GDPR', 'benefits', 'modeling', 'collaboration today', and 'barriers'. In the second coding cycle, we refined the 'benefits' and 'barriers' codes. By analyzing and comparing the text segments of these codes in detail, we derived sub-codes to receive a higher precision. We distinguished between 'benefits of EAM for GDPR implementation' and vice versa. For example, frequent sub-codes of 'benefits of GDPR implementation for EAM' were 'reinforcing EAM's value contribution' and 'increasing awareness of EAM'. In the third coding cycle, all codes were reviewed and, if applicable, refined and reorganized. For instance, we recoded some text segments previously coded as 'modeling' as the sub-code 'complexity of EA models', being part of the code 'barriers'. In addition, we integrated some infrequent, but essential sub-codes into broader sub-codes using axial coding [37]. In total, we had a final list of 1,671 coded text segments.

3.3. Induction and evaluation

In the third step, we derived design principles for EAM, which are "general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission" [24]. We referred to our empirical insights, especially to the benefits and barriers identified, to inductively derive design principles that shall foster EAM to enhance information governance. To infer the principles in a structured way, we followed Greefhorst and Proper [38], who propose that design principles in EAM research are best specified by (1) a clear statement of the principle that succinctly defines the rule, (2) the rationale behind that statement to highlight the benefits, and (3) the implications that follow to clarify the needed requirements. In a fourth step, we discussed the validity and generalizability of the derived principles during a focus group [15] with five EAM experts from one of the world's largest e-commerce companies, whom we had not interviewed before, for a preliminary evaluation. We broke the principles down in their structure, applicability and completeness. The experts generally agreed with the principles as guidance for EAM to enhance information governance and reflected a similar situation as the one we identified through our empirical study. Nevertheless, the statements, rationales and implications were refined together with the experts to ensure a higher preciseness.

4. Results

In the following, we present the results of our study by describing the identified mutual benefits of EAM and the GDPR (RQ1), the barriers of EAM in supporting GDPR implementation (RQ2) and the derived design principles that organizations should consider to foster EAM for enhancing information governance (RQ3).

4.1. Mutual benefits of EAM and the GDPR

In our empirical data, we found several explanations on how EAM and the GDPR enrich and reinforce each other. Table 2 starts by showing the nine most frequently mentioned benefits of EAM for GDPR implementation and their absolute frequency in the 24 interviews.

Table 2. Benefits of EAM for GDPR implementation

No.	Description	Frequency	
O1.1	Enables the reuse of existing EA models to create and update the record of processing activities	19	79%
O1.2	Provides a central point of contact for information acquisition of the data protection officer	15	63%
O1.3	Increases sustainability of documenting privacy aspects in business, IT and information artifacts	13	54%
O1.4	Supports fulfilling the rights of data subjects	12	50%
O1.5	Fosters a common terminology in an organization	10	42%
O1.6	Simplifies privacy impact assessments when evaluating and implementing new technologies	7	29%
O1.7	Allows a self-reporting on needed EA information by the data protection officer through EA tools	6	25%
O1.8	Improves impact assessments of data breaches	4	17%
O1.9	Supports the implementation of privacy by design	4	17%

In 19 of the 24 interviews, the respondents underlined the reuse of information from existing EA models as a great relief to create the record of processing activities (O1.1), which requires to document all applications used to process personal data [5, Art. 30]. An interviewee specified: *"The people here are so happy that they invested in EAM to create basic overviews. I mean, the EA models inform us about all applications. I know exactly which application uses which data and where to designate a processing activity"* (I10). Other participants declared that the EAM department provides a central point of contact for the data protection officer to get specific information needs continuously satisfied (O1.2). This reduces the effort for the data protection officer to collect and aggregate information from all departments. In addition, 54% noticed that EAM is indispensable to guarantee a sustainability of documentation obligations (O1.3), such as the record of processing activities. I8 mentioned: *"When the date 'examination is due' comes again, then everyone will run again hectically, but of course this is not a good way to proceed. Overall, I would say that EAM not only can, but it must be part of implementing the GDPR, especially to ensure a lasting sustainability of privacy-relevant information."* Half of the respondents acknowledged that EAM is helpful in complying with the rights of data subjects (O1.4). For instance, EA models provide transparency on the storage location of personal data by tracing back its flow across applications and processes. Thereby, specific personal data can be corrected, erased or transmitted more swiftly at the request of data subjects [5, Art. 16, 17, 20]. The interviewees also stated that EAM fosters a common use of terms and an equal understanding of business, IT and information artifacts (O1.5). This prevents confusion and ambiguities between employees of analytics, privacy, security and other departments. Moreover, EA models support privacy impact assessments (O1.6), which have to be carried out when a new type of processing, such as the integration of a new application, is likely to entail a high risk for the privacy of data subjects [5, Art. 35]. A respondent clarified: *"When a new product comes into the house, the EA model helps us to do a conformity test. It facilitates the integration, even if it is only roughly modeled. We can predict dependencies, assess risks, and evaluate how it meshes with personal data and whether it complies with our privacy policy"* (I6). A quarter of the experts also indicated the usefulness of EA tools for self-reporting (O1.7). I20 stated: *"If the data protection officer had self-reporting to get privacy information out of the EA tool, it could certainly help him to regularly check privacy-relevant aspects or to answer questions, such as: Are all relevant applications considered in the record of processing activities?"* The respondents also recognized that transparency through EA models helps to assess the impact of data breaches and to create related notifications (O1.8), which require a description of the cause, extent and consequences of the data breach [5, Art. 33]. Other interviewees admitted that EAM is interlinked with their security departments. By assigning security-related attributes to the artifacts in EA models, the realization of technical and organizational measures for privacy by design can be supported (O1.9).

Conversely, Table 3 now gives an overview of the most significant benefits of GDPR implementation for EAM according to our respondents.

Table 3. Benefits of GDPR implementation for EAM

No.	Description	Frequency	
O2.1	Strengthens the value contribution of EAM	23	96%
O2.2	Leads to more complete and updated EA models	20	83%
O2.3	Intensifies EAM's collaboration with departments	20	83%
O2.4	Increases organizational awareness of EAM	16	67%
O2.5	Enables discovery of potentials by enriched models	15	63%
O2.6	Fosters EAM in consolidating the IT landscape	9	38%
O2.7	Expands EAM's tasks to other digital challenges	7	29%
O2.8	Provides a lever for EAM to manage shadow IT	4	17%
O2.9	Improves portability of EAM to other regulations	3	13%

Nearly all interviewees observed that the GDPR not only legitimizes, but also boosts the value contribution of EAM in their organization (O2.1). Summing up, they stated that the GDPR substantially strengthens EAM's position, enables EAM to further develop its potential and expands EAM's scope. A respondent stated: *"By considering topics like big data and GDPR, the EAM discipline is enforced outside the IT and increasingly perceived as an important key player. That is why the issue of privacy is very attractive for EAM, because it cannot be swept under the carpet"* (I2). In addition, the interviewees declared that the GDPR implementation leads to more precise EA models (O2.2), as the data layer has gained in importance and data flows between EA artifacts are captured more accurately. This is closely related to the next opportunity, namely that the GDPR strengthens the collaboration between EAM and other departments (O2.3). According to the respondents, the GDPR causes employees of business and IT departments to have new information needs, but at the same time also drives them to work proactively with EA tools and to maintain EA models by themselves. I7 summarized this interplay as follows: *"From an architectural point of view, the problem is always that models become obsolete. This can be counteracted: the more persons use the model, the more updated it remains. The GDPR is thus a huge advantage for the EA model. In addition, the end-users, including the data protection officer, have huge advantages because they have an updated model and save a lot of work."* 67% of the participants also stated that the GDPR increases EAM's awareness level in an organization as a whole (O2.4). Two enterprise architects mentioned: *"The GDPR gave us a nice boost. Now, more people need insights into organizational structures and associate this with EAM"* (I18). *"The GDPR emphasizes that EA is not just pure documentation for the filing cabinets. Until now, the thought was often that EAM is only something for the archives"* (I22). In addition, the respondents reported that enriched EA models now help *"to recover and appraise existing or hidden treasures"* (I2), as a more fine granular transparency of capabilities, applications, data objects and flows reveals potentials, especially in the context of big data analytics (O2.5). For example, if a particular process is supplemented with insights from aggregated personal data, another similar process may be improved as well. The interviewees also added that the GDPR enforces EAM to leverage a cleanup of the IT landscape (O2.6). A participant stated: *"The GDPR gave us the possibility to consider other relevant aspects and to trigger improvements that apply to the entire application and process landscape"* (I18). Moreover, the GDPR increases EAM's scope to support tasks like data qualification and data management, but also topics like agility and outsourcing (O2.7). Other participants underlined the importance of the GDPR in supporting EAM *"to achieve transparency of the IT landscape, in particular regarding the shadow IT. We found out that the shadow IT is at least as powerful as the governed IT"* (I16) (O2.8). As creating the record of processing activities requires substantial transparency, the GDPR is a lever to move the shadow IT into light. Three experts added that enriched EA models and an improved interplay of EAM and other departments are valuable to comply with other regulations as well (O2.9).

Overall, our study revealed multiple benefits of how EAM and the GDPR enrich each other. While EAM especially supports GDPR implementation through its overarching view on the integration of the information artifact in an organization, the GDPR increases EAM's value contribution and the timeliness of EA models. In addition, EAM can be an enabler for sustainable GDPR compliance, whereas the GDPR increases the interplay of EAM with other departments and improves the EAM awareness throughout an organization.

4.2. Barriers of EAM in supporting GDPR implementation

Besides the multitude of benefits identified, our empirical data also revealed current barriers of EAM in supporting the implementation of the GDPR. Although the industry and in particular the size of organizations can be assumed to have a great influence on the intensity of the barriers, the selected heterogeneity among the organizations interviewed did not reveal significantly different barriers. We thereby could ensure an adequate level of generalizability, while receiving representative results across the interviews. Table 4 summarizes the major barriers mentioned by our respondents.

Table 4. Barriers of EAM in supporting GDPR implementation

No.	Description	Frequency	
B1	Maintenance and timeliness of EA models	24	100%
B2	Lack of institutionalized information exchange	21	88%
B3	Inaccurate granularity and content of EA models	19	79%
B4	Divergent understanding between departments	15	63%
B5	Separate tools and redundant data collection	13	54%
B6	Unclear responsibility and tasks of EAM	11	46%
B7	Organizational anchoring and IT focus of EAM	7	29%
B8	Low familiarity and habit of interaction with EAM	7	29%
B9	Historically caused bad image of strict rules	5	21%

All interviewees underlined the effort required to maintain and update EA models and perceived this to be the greatest barrier currently (B1). Although the GDPR contributes to a better quality of EA models (O2.2), also through autonomous updates by the departments (O2.3), the effort and required level of detail still outweigh. In large organizations and across locations it is exceedingly challenging to sustainably document the high number of applications, data objects and data flows. An expert surveyed mentioned: *"I think the main problem at the moment is the maintenance effort. With data acquisition and modeling tools, the motto is 'all or nothing'. Either you maintain the models really well and up-to-date, then they are very valuable, but as soon as the data quality decreases, you can no longer trust them"* (I12). Other experts complained that digital technologies, especially cloud computing, cause incomplete models and shadow IT: *"We have to model many things as black boxes. If we use an Azure service to get customer insights, we cannot exactly comprehend what is happening in the background"* (I20). *"When a department simply rents a cloud or installs something without saying anything, this leads to gaps"* (I22). In addition, the respondents stated that the information exchange between EAM and other departments is rather rudimentary (B2), although the GDPR has already led to an improvement (O2.3, O2.4). They said that meetings to receive EA information have become more frequent, but are still too uncommon to have continuously updated EA models. I12 mentioned: *"The response rate is not 100%. You always have to run after them or contact the application owners individually to get the required information."* The third barrier refers to the difficulty of achieving the right level of detail in EA models (B3). In today's data-driven businesses, this challenge is further increasing as the information artifact and its storage, transmission and processing, have to be captured. Therefore, EA models need to be tailored even more accurately than before to respond to the specific information needs of stakeholders, e.g., those of the data protection officer. An interviewee summarized: *"We are not capable of modeling an entire company anymore. In such a complex environment, we can no longer manage that. Today, you need small models that answer precise questions"* (I1). However, receiving precise questions and understanding the information needs of stakeholders is very difficult for the EAM, as other departments often have a divergent understanding of the architecture (B4). A respondent illustrated the situation as follows: *"What worries me or what we have to ensure is that everyone is talking about the same things. If we mean application A, it also has to be application A in service management, in IT controlling and in the privacy department. This is a big challenge today, because in times of many cross-divisional functions and increasing agility, everyone is a little bit on his own"* (I1). Half of the experts also said that their organizations started GDPR preparation rather late. Needed EA information, such as applications, was extracted from EA tools at short notice, entered again in rudimentary tools or Excel tables and complemented with privacy-related information. This led to a cycle that causes unnecessary effort and redundant data collection (B5), since many EA tools, such as LeanIX, provide fundamental GDPR compliance functions and seem to be more adequate to ensure sustainability (O1.3). I8 stated: *"Unfortunately, a lot of privacy information does not arrive in our EA tool yet. Too little governance was done. We should have intercepted that earlier."* Further, in many organizations EAM's responsibility on the topic is not regulated (B6). The interviewed experts admitted that they are not entirely clear to what extent they have to support analytics, privacy and security departments, as tasks arise more or less spontaneously and therefore often cannot be performed directly. This is closely linked to the fact that EAM's position in organizations is still rather IT focused (B7) and that many departments have a low habit of collaboration with EAM (B8). Even though the GDPR increases EAM awareness (O2.4), many departments are unfamiliar with EAM and do not proactively provide required information or engage with EAM. The respondents also added that EAM still has an image problem, as it is often seen as a rigid function consisting of strict rules with lethargic documentation tasks and is only for specialized architects (B9).

Summing up, we observed that particularly the effort required to maintain EA models and the lack of constant collaboration prevent a more extensive support of GDPR compliance by EAM. To create value, EA models also have to be aligned more closely with information needs.

4.3. Design principles for EAM to enhance information governance

From the benefits and barriers, we derived seven design principles that shall guide organizations to foster EAM in supporting information governance, especially the task of GDPR implementation, but also tasks like data governance and improving information usage. We argue that EAM can learn from the organizations' need of GDPR compliance to take today's data-driven nature into account. Table 5 gives an overview of the principles.

Table 5. Design principles for EAM to enhance information governance

Type	No.	Design principle	Rationale by GDPR implementation	Main implications for EAM
Structural	DP1	Identify the decision-makers within information governance to prioritize the customers of EAM	- Need to clarify EAM's organizational position and main customers (mainly O1.6, O2.1, O2.4, O2.5, O2.7, B6-B9)	- Balance priorities of customers, e.g., information strategy committee, data protection officer - Foster an understanding of architectural relations
	DP2	Define roles and responsibilities in each department that collaborate with EAM on managing the information artifact	- Need to regularly update EA models (mainly O1.1-O1.4, O1.6-O1.9, O2.2, O2.5, O2.6, O2.8, B1, B3, B5)	- In each department, assign the role "information architect" to representatives as contact for EAM - Control that the role is continuously performed
Procedural	DP3	Foster strategy development regarding information usage by providing valuable insights into architectural relations and potential synergies	- Need for EAM to leave the ivory tower and become a more embedded consulting function (mainly O1.6, O2.1, O2.4, O2.5, O2.7, B6-B9)	- Highlight dependencies on the information artifact by providing simple visualizations of EA models - Support decision-makers in maximizing information value by revealing gaps in information usage
	DP4	Proactively advise all business and IT departments in realizing effective information governance	- Need to support all departments in managing information (mainly O1.4, O1.6-O1.9, O2.1, O2.3-O2.9, B6-B9)	- Assist departments in minimizing and protecting data by clarifying key interrelations of data objects - Foster departments to improve information quality
Relational	DP5	Ensure a shared terminology and unified definitions of the EA in the context of information governance	- Need for a common understanding of the EA (mainly O1.3, O1.5, O1.9, O2.2-O2.4, O2.9, B1, B2, B4)	- Align definitions of EA artifacts with those used in analytics, security and privacy departments - Negotiate a joint terminology and reach a consensus
	DP6	Create and use a lean and intelligible EA meta-model that covers information artifacts, data flows and data processing	- Need to diffuse EA models and extend them by information artifacts (mainly O1.1, O1.3, O1.4, O2.2, O2.5, B1, B3)	- Extend EA meta-model by information artifact - Enable non-architects to understand EA models by keeping them accessible, simple and visualizable
	DP7	Initiate a routine for information exchange and the use of a shared EA repository for information governance	- Need to integrate EA information and EA stakeholders (mainly O1.2, O1.6, O1.8, O2.1- O2.3, O2.9, B2, B6, B8)	- Incentivize by promoting the benefits of EAM - Arrange continuous meetings to receive up-to-date EA information and needs of relevant stakeholders

To structure the design principles and to clarify how EAM can contribute to information governance, we refer to the three types of practices of IT governance [16], as they can be adopted to information governance [18].

Structural: Being a relatively unexplored topic, the roles of information governance are not exactly defined. Thus, as a first principle, we propose that EAM must identify and prioritize its main customers in the context of information governance, e.g., executives responsible for decision-making on information usage, data analysts or data protection officers (DP1). Thereby, EAM can legitimize its position and key tasks within information governance. To ensure timeliness and completeness of EA models, which are intended to provide transparency on information integration throughout an organization within information governance, representatives have to be assigned in each department that closely collaborate with EAM (DP2). Having the role of an "information architect", these representatives should regularly report on current information needs, make organizational and technical changes of their department transparent and highlight current limits of information usage.

Procedural: Based on its unique and fully integrated vantage point of information usage along all architectural layers of an organization, EAM is able to contribute to strategy development and decision tasks on information usage (DP3). By comparing and analyzing information needs and specifying EA models and visualizations for analytics, privacy, security and other departments, EAM can reflect the current situation of information usage and its relationship with all business and IT artifacts and give advice to decision-makers for future planning. As EA models often tend to be complex and not directly understandable for non-architects, simple visualizations of gaps and potential synergies of information usage should be presented instead. In addition, EAM should use its comprehensive knowledge on organizational and technical relations to take a more proactive position and support other departments in managing the information artifact (DP4). For example, EAM can elucidate which core processes, services and applications along multiple departments are dependent on what type of data and thereby assist in erasing or protecting specific data. In addition, when capturing the information artifact and its flows, EAM is able to highlight relations to big data analytics processes, to reveal redundant data collection and to support an improvement of data quality.

Relational: As a basis for the procedural practices, EAM should follow a set of design principles that enable relational practices to enhance information governance architecturally. First, EAM should negotiate a shared terminology of business, IT and information artifacts with the departments, especially those representing key functions relevant for information governance, such as analytics, security and privacy, to ensure a common understanding and to avoid ambiguities (DP5). Without an alignment of definitions, confusion about information needs might occur and, consequently, provided models and visualizations do not meet the demand. Second, an EA meta-model is needed that covers aspects relevant for information governance, e.g., information artifacts and flows as well as attributes that address security and privacy issues (DP6). Such a meta-model should provide a basis for a shared and integrated repository of EA information and prevent redundant efforts on achieving transparency. For example, additionally to the security department, privacy departments require transparency on security measures as well to check and manage compliance with privacy by design requirements [5, Art. 25]. Burmeister et al. [6] provide an example for such a meta-model, but the interviewees stated that this meta-model is rather too complex for maintenance in practice, although it might be complete from a scientific point of view. Instead, an EA meta-model should be kept simple and cover key artifacts and attributes needed. Third, a regular exchange of information with the "information architects" mentioned in DP2 is unavoidable to update the EA repository and to understand current information needs of the departments (DP7). While most of the respondents remarked the lack of such a routine, the experts we consulted for evaluation of the principles reported on a three-month period in their organization for discussing EA information with other departments and confirmed the effectiveness of closer collaboration.

5. Discussion and conclusion

Despite the increasing importance of information governance efforts [1, 2, 9], recent surveys acknowledge inconsistent collaboration of organizational departments on managing information and a continued reliance on siloed, ad hoc processes [14, 21]. Moreover, compliance with regulations like the GDPR force organizations to be completely transparent on information integration. To this end, EAM can be a key for information governance by revealing how the information artifact flows along all layers of EA. The results we received by conducting 24 interviews with EAM experts reveal many benefits of a close interplay of EAM and GDPR implementation, but also underline important barriers, especially the effort to maintain EA models and the insufficient collaboration with EAM departments. Thus, we derived seven design principles for EAM that provide guidance to harness the identified benefits and to overcome the barriers.

From an academic perspective, our results contribute to the research gap on integrating EAM and information governance. While research on this topic is scarce and focuses on architectural models that cover aspects of security or privacy [6, 27, 28], our results empirically elucidate the current interplay and provide principles for structural, procedural and relational practices to support a closer integration of these two domains. Moreover, our study confirms previous findings on the organizational challenges in realizing EAM. In accordance with the study of Hauder et al. [12] from 2013, the organizations in our sample validate that EAM is still characterized by an insufficient information exchange and is perceived to be rather IT than business focused. Moreover, we extend this list by revealing the specific barriers of EAM in supporting GDPR implementation. While our results empirically confirm the need to closer align EAM with aspects of analytics, security and privacy, as highlighted by several scholars [6, 26, 28], they also underline that EAM as an organizational function and its architectural models have to be more lightweight and pragmatic in order to create more value for other departments. This complies with the idea of architectural thinking, which is about moving EAM forward to a less formalized and utility-centered approach to support non-architects and people outside the IT function to understand, transform and communicate fundamental structures [25]. Against this background, our design principles can be seen as a guideline to initiate architectural thinking in the context of information governance. However, research needs to define the structural, procedural and relational practices of information governance to exactly determine how EAM or architectural thinking can contribute to realizing effective information governance. Moreover, our results implicate the close relation of information governance and IT governance using the example of implementing the GDPR. For instance, GDPR compliance requires a more complete transparency on the shadow IT, giving IT governance opportunities to manage the shadow IT. This indicates that our design principles provide benefits for IT governance as well, as transparency on information integration by EA models supports decision-making on IT investments. The results also relate to the discussion about the IT artifact's position in ISR. For instance, Lee et al. [39] distinguish between technical, information and social artifacts. While EAM is often perceived to focus on the technical or physical IT artifact, our results incite EAM to consider the information artifact more intensely.

For practice, the results support organizations in recapitulating their current situation on realizing GDPR compliance and in recognizing the benefits, but also barriers in using EAM for GDPR implementation. In addition, the design principles guide organizations in achieving a closer alignment of EAM and information governance, particularly for the topical task of GDPR implementation. Above all, the empirical insights given by our study incite organizations to take advantage of EAM for achieving a comprehensive transparency on information integration in order to balance the increasing dependence on data with privacy requirements.

The results of this paper are not without limitations. First, we conducted the interviews only with enterprise architects. Considering the perspective of other roles, such as the data protection officer, might have revealed additional benefits and barriers and led to other design principles. Second, we examined the interplay of EAM and information governance solely by using the example of GDPR implementation. Studying how EAM supports other related aspects, e.g., big data analytics, could have shed a different light on EAM's value contribution and completed our findings. Third, many companies are still in progress of becoming completely GDPR compliant, why our results merely represent a current snapshot of how EAM and the GDPR influence each other. Hence, the design principles do not claim to cover completeness, but rather provide first steps towards a closer integration of EAM and information governance.

Additional research is required to define the exact notion of information governance and to understand its interrelation with EAM. Our future work will focus on validating the design principles in practice and on refining them by other tasks of information governance.

6. Acknowledgments

This work was sponsored by the Hamburg Ministry of Science, Research and Equality under the reference LFF-FV 34 and the German Federal Ministry of Education and Research (BMBF) grant 01IS17049 / UMEDA.

7. References

[1] P. P. Tallon, R. V. Ramirez, and J. E. Short, “The Information Artifact in IT Governance: Toward a Theory of Information Governance”, *JMIS*, 30(3), 2013, pp. 141-178.
[2] R. F. Smallwood, *Information Governance: Concepts, Strategies, and Best Practices*, Hoboken, NJ: Wiley, 2014.
[3] World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011.
[4] Statista, *Big Data Analytics Revenue worldwide 2015-2022*, https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/, accessed May 15 2019.
[5] European Union, “General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council”, *Official Journal of the European Union*, 111, 2016, pp. 1-88.
[6] F. Burmeister, P. Drews, and I. Schirmer, “A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation”, *Proceedings of the 52nd HICSS*, Wailea, USA, 2019, pp. 6052-6061.
[7] L. Kappelman, R. Torres, E. McLean, C. Maurer, V. Johnson, and K. Kim, “The 2018 SIM IT Issues and Trends Study”, *MIS Quarterly Executive*, 18(1), 2019, pp. 51-84.
[8] T. Hulme, “Information Governance: Sharing the IBM approach”, *Business Information Review*, 29(2), 2012, pp. 99-104.
[9] M. N. Kooper, R. Maes, and E. E. O. Roos Lindgreen, “On the governance of information: Introducing a new concept of governance to support the management of information”, *International Journal of Information Management*, 31(3), 2011, pp. 195-200.
[10] J. Hagmann, “Information governance – beyond the buzz”, *Records Management Journal*, 23(3), 2013, pp. 228-240.
[11] K. D. Niemann, *From Enterprise Architecture to IT Governance: Elements of Effective IT Management*, Wiesbaden, Germany: Vieweg, 2006.
[12] M. Hauder, C. Schulz, S. Roth, and F. Matthes, “Organizational factors influencing enterprise architecture management challenges”, *Proceedings of the 21st ECIS*, Utrecht, The Netherlands, 2013.
[13] T. T. Lajara and A. C. G. Maçada, “Information Governance Framework: The Defense Manufacturing Case Study”, *Proceedings of the 19th AMCIS*, Chicago, USA, 2013.
[14] Compliance, Governance and Oversight Council, *CGOC Information Governance Benchmark Survey Report*, 2018.
[15] M. D. Myers and M. Newman, “The qualitative interview in IS research: Examining the craft”, *Information and Organization*, 17(1), 2007, pp. 2-26.
[16] S. De Haes and W. Van Grembergen, “IT Governance and Its Mechanisms”, *Information Systems Control Journal*, 1, 2004, pp. 27-33.
[17] P. Mikalef, J. Krogstie, R. van de Wetering, I. O. Pappas, and M. N. Giannakos, “Information Governance in the Big Data Era: Aligning Organizational Capabilities”, *Proceedings of the 51st HICSS*, Waikoloa, USA, 2018, pp. 4911-4920.
[18] K. Weber, B. Otto, and H. Österle, “One size does not fit all: A contingency approach to data governance”, *Journal of Data and Information Quality*, 1(1), 2009, pp. 1-27.
[19] P. Weill and J. W. Ross, *IT Governance*, Boston, MA: Harvard Business School Press, 2004.
[20] V. Khatri and C. V. Brown, “Designing Data Governance”, *Communications of the ACM*, 53(1), 2010, pp. 148-152.
[21] Cisco, “Maximizing the value of your data privacy investments – Data Privacy Benchmark Study”, 2019.
[22] ISO/IEC/IEEE, “Systems and software engineering – architecture description”, *ISO/IEC/IEEE 42010:2011*.
[23] R. Winter and R. Fischer, “Essential Layers, Artifacts, and Dependencies of Enterprise Architecture”, *Journal of Enterprise Architecture*, 3(2), 2007, pp. 7-18.
[24] The Open Group, *TOGAF Standard*, version 9.2, 2018.
[25] S. Aier, N. Labusch, and P. Pähler, “Implementing Architectural Thinking: A Case Study at Commerzbank AG”, *Trends in Enterprise Architecture Research*, Berlin/Heidelberg, Germany: Springer, 2015, pp. 389-400.
[26] S. H. Kaisler and F. Armour, “15 Years of Enterprise Architecting at HICSS: Revisiting the Critical Problems”, *Proceedings of the 50th HICSS*, Waikoloa, USA, 2017, pp. 4807-4816.
[27] G. Karjoth, M. Schunter, and M. Waidner, “Privacy-enabled services for enterprises”, *Proceedings of the 13th DEXA*, Aix-en-Provence, France, 2002, pp. 483-487.
[28] M. Shariati, F. Bahmani, and F. Shams, “Enterprise information security, a review of architectures and frameworks from interoperability perspective”, *Procedia Computer Science*, 3, 2011, pp. 537-543.
[29] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, “Action Design Research”, *MIS Quarterly*, 35(1), 2011, pp. 37-56.
[30] A. R. Hevner and S. Chatterjee, *Design Research in Information Systems*, New York, NY: Springer, 2010.
[31] S. Gregor, “The Nature of Theory in Information Systems”, *MIS Quarterly*, 30(3), 2006, pp. 611-642.
[32] D. Stelzer, “Enterprise Architecture Principles: Literature Review and Research Directions”, *Service Oriented Computing*, Berlin/Heidelberg, Germany: Springer, 2010, pp. 12-21.
[33] T. Widjaja and R. W. Gregory, “Design Principles for Heterogeneity Decisions in Enterprise Architecture Management”, *Proceedings of the 33rd ICIS*, Orlando, USA, 2012, 11 pages.
[34] G. L. Richardson, B. M. Jackson, and G. W. Dickson, “A Principles-Based Enterprise Architecture: Lessons from Texaco and Star Enterprise”, *MIS Quarterly*, 14(4), 1990, pp. 385-403.
[35] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, “A Design Science Research Methodology for Information Systems Research”, *JMIS*, 24(3), 2007, pp. 45-77.
[36] P. Mayring, “Qualitative Content Analysis”, *Forum: Qualitative Social Research*, 1(2), 2000.
[37] J. Saldaña, *The Coding Manual for Qualitative Researchers*, Thousand Oaks, CA: Sage, 2015.
[38] D. Greefhorst and E. Proper, *Architecture Principles: The Cornerstones of Enterprise Architecture*, Springer, 2011.
[39] A. S. Lee, M. Thomas, and R. L. Baskerville, “Going back to basics in design science: from the information technology artifact to the information systems artifact”, *Information Systems Journal*, 25(1), 2015, pp. 5-21.