Empirical Results on the Collaboration Between Enterprise Architecture and Data Protection Management during the Implementation of the GDPR

Dominik Huth[1], Fabian Burmeister[2], Florian Matthes[1], Ingrid Schirmer[2]
[1]Technical University of Munich, [2]University of Hamburg
{dominik.huth, matthes}@tum.de, {burmeister, schirmer}@informatik.uni-hamburg.de

Abstract

The European General Data Protection Regulation's (GDPR) large imminent fines cause companies worldwide to undertake major efforts for privacy compliance. Any company doing business with European customers has to adhere to new processing principles and documentation requirements, and provide extensive access rights to data subjects.

Enterprise architecture management (EAM) provides a theoretical and methodical framework to align business and IT and has been used, among others, to identify and address concerns that arose from regulation.

In this work, we report results from 24 qualitative interviews with 29 enterprise architects on how EAM supports the work of data protection management (DPM) experts. We derive a conceptual framework with four different levels of EAM support for DPM, and discuss high-level recommendations for each level.

1. Introduction

Since the introduction of the GDPR [1], companies worldwide have been alarmed by the fines of up to 4% revenue per incident. The biggest fine to date has been $50 million for Google in France for the lack of transparency [2] - an unprecedented figure that underlines that the GDPR cannot be ignored and appropriate measures have to be established. According to an industry study from 2018 [3], 68% of companies with 500 or more employees have spent over $100,000 on GDPR implementation before May 25, 2018 and 87% expect privacy to become even more important after the passing of the GDPR deadline.

The tasks for becoming compliant with the GDPR are manifold and interdisciplinary. The UK's Information Commissioner's Office lists *lawfulness, fairness and transparency*, *individuals' rights*, *accountability and governance*, and *data security, international transfers and breaches* as the top categories in a self-assessment tool [4]. Tikkinen-Piri et al. identify twelve key implications for data intensive companies to become compliant with the GDPR [5]. We reorganize these implications as tasks in Table 1.

Table 1. GDPR tasks, based on [5].

ID	Task
T1	*Purpose:* Specifying data needs and usage
T2	*Documentation:* Maintaining documentation and demonstrating compliance with GDPR requirements
T3	*Data breaches:* Developing processes to deal with data breaches
T4	*Data protection:* Data protection by design and default
T5	*Processing agreements:* Conditions for data processing in international/national context
T6	*Data subject rights:* Obtaining consent on personal data usage, ensuring individuals right to be forgotten and the right to data portability
T7	*Risk management:* Reckoning with sanctions for non-compliance
T8	*Assign responsibilities:* Designating a data protection officer (DPO)
T9	*Inform data subjects:* Providing information to data subjects

The function that we term *data protection management (DPM)* is responsible for fulfilling these tasks. DPM is headed by the data protection officer (DPO) and is often part of the legal department. As an industry study reports, practitioners perceive the overall complexity of the regulation as the biggest challenge in GDPR implementation efforts [3]. The interdisciplinary nature of the tasks between legal, business and IT means that various departments are involved and a full overview of the company is needed. Complex digital business models make this task even harder, especially in large organizations.

Enterprise Architecture Management (EAM) aims to strategically develop the IT and business architecture of a company.[1] The function addresses a broad range of concerns, for example the identification of data flows, and provides a common language of methods and visualizations to achieve these purposes [7]. Among IT and EAM experts, 67% name cross-organizational collaboration as a benefit of EAM, and 65% of respondents see EAM as an enabler for transparency [8]. A survey from 2015 ranks (general) regulatory requirements as the most relevant influence factor on EAM [7].

In this work, we aim to investigate the contribution of EAM during the preparation phase for the GDPR. We define the following research questions:
RQ1: *How do EA practitioners support data protection management in the fulfillment of GDPR requirements?*
RQ2: *Which different levels of collaboration exist?*
RQ3: *What are the prerequisites for EA to support these levels of collaboration?*

To this end, we interviewed 29 EAM experts from 24 organizations in the German-speaking area for their collaboration with DPM. The remainder of this work is organized as follows: We present related work in section 2. Section 3 presents our conceptual model of EA support for GDPR tasks that we developed from the interviews. High-level recommendations for each level are given in section 4. We conclude this work and discuss future research directions in section 5. The appendix presents our research approach and a characterization of the interview partners.

2. Related work

Given that the GDPR came into effect in 2018, there are still few scientific contributions on the interplay between EAM and DPM. In particular, we are not aware of any empirical work on privacy aspects in EAM and aim to address this research gap. We first summarize work on EAM and IT security or privacy. We then present theoretical approaches how EAM can contribute to GDPR compliance.

2.1. Enterprise security architecture and enterprise privacy architecture

Innerhofer-Oberperfler and Breu present a model-driven approach for enterprise security management using EA [9]. The challenges they identify refer to the complexity of business processes with their dependencies and interrelationships, the support of stakeholders, identifying the right level of abstraction for security-related information, and establishing a continuous process for security management. The authors present a detailed meta-model of security information and develop a security management process that involves the adaptation of the EA model, the definition of business security objectives, identification of dependencies, a risk and threat analysis, engineering security controls and the reiteration of the process. The identified risk assessments are then aggregated in higher levels of abstraction.

Grandry et al. map concepts of information security risk management to the ArchiMate modeling language [10]. The approach makes it possible to identify business and IT assets for which information security assessments are required. However, the modeling approach does not directly allow expressing relationships between risks and the assessed elements. The authors conclude that the integration of EA and risk management is necessary for a company's ability to manage risks.

A white paper by Ann Cavoukian, initiator of *Privacy by Design (PbD)*, and Oracle assesses how PbD and EA can realize a security by design approach [11]. The authors propose an enterprise-level process evaluating the current security capability maturity, identifying gaps between the current and the desired state and defining a strategic roadmap for filling the gaps. To ensure sustainable implementation of PbD in EA, a strong EA governance process in harmony with the proactive PbD principles should be established.

2.2. Enterprise architecture management and GDPR

Rozehnal and Novak argue that EA supports SMEs in addressing concerns of the GDPR [12]. They point out the benefits of knowing the internal structure of a company and describe the line of analysis *function*, *data*, *process*, *application*, *people* and *technology*. However, as we observed in the interviews, such complete EA models typically do not exist in practice.

Burmeister et al. assign GDPR articles to four categories of requirements: *compliance with superior principles*, *information obligations*, *data subject rights* and *implementation and verification of technical and organizational measures* [13]. For each category, a list of relevant EA elements at different EA layers is given. The paper then presents an EA meta model that addresses the information requirements of the GDPR.

Other work presents a viewpoint that describes software architectures from a data protection perspective [14]. By using data flow diagrams, the authors bridge the dichotomy between legal reasoning, e.g.

[1] ISO defines enterprise architecture 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."* [6].

in data protection impact assessments (DPIA), and an engineering perspective. In the construction of the view, the authors refer to the importance of a consistent terminology and the right level of abstraction. According to Basin et al., an interprocess data flow model is necessary to audit GDPR compliance [15]. The authors model processes in BPMN, because each business process represents one or more purposes for data processing. A formalization allows for semi-automated compliance checks of implementations to process models, process models to GDPR requirements, process models to privacy policies, or privacy policies to the GDPR.

Further contributions address the DPIA by describing a process and possible evaluation criteria from a practical point of view [16], processes for creating a record of processing activities [17], or a service definition for data portability [18].

3. Tasks

We identified eight different tasks that enterprise architects conducted or supported during the GDPR implementation phases and organized them into the four levels *usage of existing information (1)*, *enriching existing information (2)*, *analysis based on EA documentation (3)* and *constructive management of EA and data protection (4)*. We describe these categories and the respective tasks, as well as practical insights, in this section.

Figure 1 shows the four levels of EA support for DPM activities from left to right. The respective EAM prerequisites that need to be available for each level of support are shown below. At the top, additional DPM activities to each level are displayed, i.e. at each level there are DPM activities that EAM does not support. We organized the four levels as increasing steps, because we consider the EAM prerequisites at the bottom to be built on one another. However, we do not consider the levels themselves to represent a maturity model, because a higher level does not require the fulfillment of all lower levels. Levels one and two have the overarching theme of providing information support, where the first constitutes a passive involvement of EAM and the second an active role. Similarly, the constructive levels three and four can be considered as analytical and specifying, respectively.

3.1. Usage of existing information

As the first level of EAM support for data protection management experts, we identified the usage of existing EA information for conducting DPM tasks. In this level, the information is handed over to DPM experts without further involvement of the enterprise architects, as confirmed by I14: *"The repository is well-suited as a point of entry, the DPM expert can get the full set of applications from there. But in the repository itself it is not evident whether an application processes personal data and thus requires special protection. The DPM expert has to investigate further in other systems that model regulatory processes"*. In the following, we discuss how the different EA elements were used to support these tasks.

One of the key responsibilities and the initial activity of any data protection documentation process is the discovery of processing activities. This is the responsibility of DPM experts, e.g. the DPO. A central result of this effort is the record of processing activities (RPA) according to Art. 30 GDPR [1]. The RPA must contain all processing activities with contact details, purposes of the processing, a description of the categories of data subjects and the processed personal data, the categories of recipients, and where possible and applicable, information about third party processors, storage limits and security measures.

The closest EA elements to processing activities are **processes**. However, detailed business processes are out of the scope of EAM and should be maintained specialized tools [19]. We also observed the limited relevance of processes among the EAM experts we interviewed. Only five interviewees explicitly had processes modeled in their repositories, but none reported that these were used as a basis for the RPA. I16 is planning to establish a direct link between processes and the RPA after reorganizing the processes.

All 21 interviewees with direct responsibility for an EA repository reported documenting the employed **applications** at the enterprise. In some cases, EA-related information was requested directly from EAM, e.g. in I01 (which information is being processed) or I11 (which information is transferred from system A to B). I12 reported that the DPM experts actively look up information in the EA repository. This was also the case for I15, but a proposal for further collaboration between EAM and DPM failed to materialize: *"I suggested to the DPO to use our repository and enhance some of the information, but I believe he still has an own perspective on this."*

Another practice was that DPM experts used a one-time export from an EA repository or a configuration management database (CMDB) without involving the enterprise architects. The DPM experts then used a survey tool to collect additional information about the applications. I08 expressed discontent with this approach, because the EA tool would have been capable of conducting the same surveys and would have

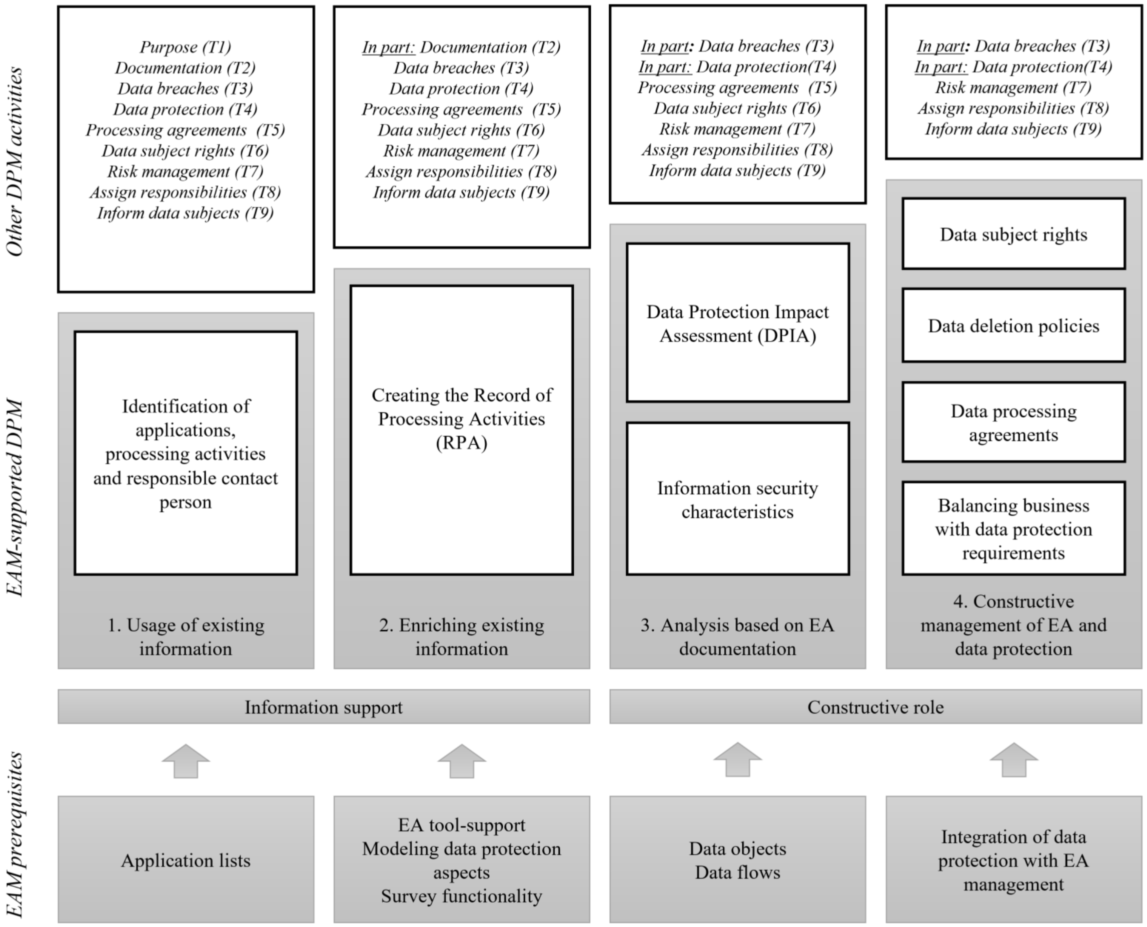
Other DPM activities
Purpose (T1)
Documentation (T2)
Data breaches (T3)
Data protection (T4)
Processing agreements (T5)
Data subject rights (T6)
Risk management (T7)
Assign responsibilities (T8)
Inform data subjects (T9)
In part: Documentation (T2)
Data breaches (T3)
Data protection (T4)
Processing agreements (T5)
Data subject rights (T6)
Risk management (T7)
Assign responsibilities (T8)
Inform data subjects (T9)
In part: Data breaches (T3)
In part: Data protection(T4)
Processing agreements (T5)
Data subject rights (T6)
Risk management (T7)
Assign responsibilities (T8)
Inform data subjects (T9)
In part: Data breaches (T3)
In part: Data protection(T4)
Risk management (T7)
Assign responsibilities (T8)
Inform data subjects (T9)
EAM-supported DPM
Identification of applications, processing activities and responsible contact person
Creating the Record of Processing Activities (RPA)
Data Protection Impact Assessment (DPIA)
Information security characteristics
Data subject rights
Data deletion policies
Data processing agreements
Balancing business with data protection requirements
1. Usage of existing information
2. Enriching existing information
3. Analysis based on EA documentation
4. Constructive management of EA and data protection
Information support
Constructive role
EAM prerequisites
Application lists
EA tool-support
Modeling data protection aspects
Survey functionality
Data objects
Data flows
Integration of data protection with EA management

Figure 1. Four levels of EAM support for DPM activities

provided a more sustainable support for these efforts. I06 only found out that such a dated list was used when receiving a survey as application owner of the EA tool. I02 also reported that a CMDB export was used for the RPA without involvement of EAM.

I03 and I20 stated that even though their EA repositories could help DPM experts in identifying relevant applications, no direct collaboration between these disciplines has taken place yet. EA documentation provides a starting point for further external activities. Thus, any kind of EA documentation may serve this purpose, regardless of its form.

3.2. Enrichment of existing documentation

The second level of support we observed was employing EA tools to enrich the existing EA documentation with necessary information for data protection management, i.e. the incorporation of DPM information requirements in an EAM process.

One variant in this level of support is **full integration** of information collection for data protection in the EA management cycle. As I04 points out, an enterprise architect knows exactly who to talk to for gathering additional information about applications. The EA repository allowed for a pre-classification to sort out applications that do not process any personal information, such as compilers, which greatly reduced the number of applications to investigate further. Our interview partner then used the survey functionality of the EA tool to send out and track a questionnaire that was designed by the information security and compliance departments.

I23 used the EA tool itself as the record of processing activities, i.e. all information about the processing activities was attached to EA model elements and the RPA is created as a report. As a reason for representing the RPA with the EA repository, I23 recalled that it provided the best starting point at the time. I22 also responded that all information that was collected during the GDPR documentation efforts is now stored in the company's EA tool, which avoids redundancy in future data collection.

Another variant is **EAM-supported information collection**. One interview partner of I16 led the overall GDPR compliance project at the company, and reported that the obligation to document processing activities goes hand in hand with the methodical approach of EAM. However, the RPA is represented in a separate tool that matches the specific needs of the DPM experts. A bidirectional interface could supply relevant information from the RPA tool to the EA tool and vice versa, but it must be clarified which system holds the leading information. I01's company documents processing activities in a Wiki and uses a one-directional interface to pre-fill the wiki pages. The main documentation of I20 is also stored in a separate resource and accessible with links from the EA tool.

I07 also advocates using the EA tool as a basic structure for data protection documentation and plans to implement an export of EA data to MS Office templates. However, I07 warns that *"we cannot reflect the whole world in our EA tool"*. Instead, the EA tool should link to external resources when necessary.

For the level *enriching existing information*, a dedicated EA tool is required. All interviewees stated that the tools they employed were able to fulfill their modeling requirements and provided the required functionalities for conducting the tasks that are related to the data collection, e.g. survey or export functionalities. Deficiencies were only seen in the usability and complexity of some EA tools, e.g. by I22. Targeted data protection views can facilitate the collaboration, because the full extent of architecture repositories could overwhelm DPM experts, as I07 noted.

3.3. Analysis based on EA documentation

An additional level of EA support for data protection management is using the existing or enriched EA documentation for information security and/or data protection analysis. We describe these two tasks separately, because information security is typically located in the IT department and data protection is usually a legal function.

An understanding of the involved data objects and the transferring interfaces is crucial for analyzing possible risks for personal data and security. However, the information has to remain at a manageable level of abstraction: I23 recounted a failed effort of a detailed classification because of too many attributes, which were then reduced by more than 80%. Attributes that were commonly used by our interviewees were whether or not an object contains personal data, the subject of the personal data (customer, prospective customer, business partner, employee), and the level of confidentiality (confidential, internal, public). Less frequently a description of the specific type of attributes, e.g. birthdate or address, was attached to the data objects. Documented interfaces also contributed to an analysis of data protection risks, as reported by I11 and I22, for example.

3.3.1. Information security. I13, speaking for a variety of EAM projects at different customers, confirmed that EA documentation can be used for identifying vulnerabilities in general. The interview partner particularly emphasized rights management and access control as tasks where EAM supports DPM.

I15 reported a coarse classification of data objects with respect to whether they represent personal information or the level of confidentiality. The company is also modeling security capabilities, such as identity management or firewalls, but with the goal of consolidating the tools that the information security departments use for these purposes. According to I15, data protection aspects are not represented in the EA repository, because it was not a requirement at the time of its initiation. According to I18, tagging objects with personal data facilitates protection requirement analysis. A similar classification of data objects was introduced by I11 during the preparation phase for the GDPR.

3.3.2. Data protection impact assessment (DPIA). The data protection impact assessment (DPIA) is an instrument to analyze which risks arise through the usage of certain technologies or processing systems [16]. The risk analysis should provide the basis for the selection and implementation of mitigation measures. The core process of conducting the DPIA comprises the identification of protection goals, the identification of potential attackers, motives and objectives, the identification of evaluation criteria and finally the evaluation of the risk [16]. With the protection goals confidentiality, integrity, availability, unlinkability, intervenability and transparency [16], we regard the DPIA as an information security evaluation *plus* data privacy.

In this context, I10 stated the goal of combining compliance processes with EAM. The DPM experts experienced a major benefit through the documentation of responsible persons, which in turn could provide information for data protection assessments. I20 also referred to the structure and terminology that EA provides, which makes the analysis of relevant applications and the definition of technical and organizational measures (TOM) for the protection of critical applications easier.

Along with I23's next step to implement an information security management system, the interviewees added that creating DPIAs for each processing activity will be a future task of the GDPR project.

3.4. Constructive management of EA and data protection

As the fourth level of EAM support for DPM, we define all activities where EAM assumes an active, enabling role in close collaboration with DPM experts. This level of collaboration requires an active discourse and frequent exchange between EAM, DPM and information security and provides further overarching benefits, such as data freshness (I07) or the groundwork for digitalization (I07, I13, I16).

3.4.1. Data subject rights. The extended data subject rights are one of the main changes that were introduced with the GDPR. They comprise the obligation to inform the data subjects how their data is processed (Art. 13, 14), the right of the data subject to access the information that is processed (Art. 15) and receive a copy in electronic form (Art. 20), the right to have personal data corrected (Art. 16) or deleted (Art. 17), and the right to restrict, as a whole or in part, processing of one's personal data (Art. 18, 21, 22).

These provisions pose considerable challenges for companies: I17 illustrated an example that the customer can now decide on a day to day basis whether or not information may be processed. This would require a consent management system that is connected to all applications that process personal data, a vision that was discussed in several interviews.

In addition to processing by multiple applications, the combination of multiple products for data subjects and multiple roles within the organization is a challenge that EA can address, as I14 stated: *"We are able to break down your customer account with all dependent contract elements. And that gives us the ability to manage access rights to your products and which employee can see what"*.

Alongside automated solutions, EAM provided a large contribution to GDPR compliance by defining processes for the data subject rights. I09 and I22 stated that there are processes for handling requests for information and for data portability. The processes specify who has to be informed and who has to be consulted. However, I22 reported that applications that are run independently by the business departments (*"shadow IT"*) remain a challenge for enterprise architects, because only the business departments know which personal data is processed there.

For complying with the right to information, I21 described the company's approach to explaining automated decisions to B2B clients, who are responsible for the processing of their customer's personal data. According to the interviewee, the exercise of data subject rights could gain more importance in the future, because the GDPR raised customers' awareness of these rights.

I16 brought up the difficulties of business departments to assess the consequences of data deletion without an overarching perspective. EAM provides a methodical approach to overcoming such limitations. I18 specifically mentioned implementation guidelines for how the right to deletion (*"right to be forgotten"*) should be implemented, but also noted that implementing the necessary steps in all applications is a lengthy process.

3.4.2. Data deletion policy. The principle of *storage limitation* (Article 5 e [1]) requires data controllers to make sure that the stored data no longer permits identification of data subjects. After fulfilling the purpose for which it was collected, it has to be deleted or anonymized. Similar to the deletion of individual data, it is a challenge to maintain the integrity of processes and to identify the leading applications for customer data. A data deletion policy specifies *"which data is kept for how long, which are the conflicting legislations, and when it can and will be deleted"* (I19).

I19 is participating in the definition of a template for data deletion policies, based on DIN Norm 66398. The template should be instantiated by application owners, who are responsible for specifying which deletion method will be used and which extent of deletion is considered sufficient. To ensure consistency, deactivation of data before deletion is an option. I11 established a process to inform the data owner of pending deletion requests and wait for approval or denial of the request. In this case, the data owner is responsible for analyzing conflicting legal requirements or the impact on the integrity of data structures.

Anonymization circumvents the problem of keeping consistency and theoretically allows further processing of the data, but as I21 remarked, anonymizing highly interconnected data, e.g. addresses, in a way that allows demographic analysis is extremely challenging. *"If you know how to maintain that distribution in your dataset, then you could also generate synthetic data."*

Another major challenge in defining a deletion policy was observed in the multiplicity of processing purposes for data objects. I14 stated: *"we have countless end to end relations between data objects, where the fact that a processing purpose for one object in no way implies the same for a dependent data object"*. For example, if the same document was used for applying for a loan and opening a checking account, the application document may not be deleted while the checking account is still open. A formal model for this case does not exist, but EAM contributes to a shared understanding and by creating a collection of metadata that lists applications, processing purposes and retention periods.

I15 referred to the regulatory requirements for the German financial and insurance industry, which also require establishing deletion policies. However, the company's information security department is responsible for implementing these in manual processes. Interview partners I06 and I08 also referred to data deletion policies as part of questionnaires that were sent out to application owners by the DPM experts, as described in section 3.1.

A notable observation for this task is that all interviewees that are subject to the German authority for financial regulation BaFin (banking and insurance) cited the current regulatory requirements in the context of deletion tasks, which indicates a high synergy potential in this field.

3.4.3. Data processing agreements. Article 28 of the GDPR lays out the conditions for third party processing of personal data. The controller is required to enter into a data processing agreement with the processor, who governs confidentiality and security of the processing, its purposes, and the obligations and liability of the processor.

I11 brought up the company's obligation to know exactly which (personal) data has been transferred to which partners. The company relies heavily on a service oriented architecture and requires all services to register in a service repository. The enterprise-wide service repository allows identification and documentation of data flows to external partners.

I22 also reported that all applications have to be registered in the EA repository in order to connect to an interface of another application. This gatekeeper function allows identifying data flows and makes it possible to oblige application owners to confirm the compliance of the application. However, the interviewee also acknowledged that applications that do not obtain data via a regular interface are not captured by this approach. The possibility to identify inter-organizational data flows through architecture models was also mentioned by I18 and I02.

3.4.4. Balancing business with data protection rights. Though it is not an obligation that arises from the regulation itself, we observed another task that enterprise architects perform in the context of the GDPR: combining the requirements of business and data protection. While it is clear that less processing of personal data reduces the risks and obligations that are related to the processing, digital business models often require exactly the opposite.

In this spirit, I09 addressed this constructive role of EA: *"At the end of the day, there is always the question how we can implement something in a way that both sides, economical success and data protection, are adequately represented"*.

An example for this was the anonymization of operational data, as reported by I15, where a personal reference is not needed. The anonymized data can then be used for general reporting and corporate management.

Similar to the analogy for privacy *"only strong brakes allow a race car to go fast"* [11], the data protection activities were even seen as an enabler for business by I16. The interviewees explained that the capability to organize data based on processes supports the capability for digitalization. The task of the enterprise architects is to spread the sensitivity for compliance within the organization and ensure sustainability in future data protection activities.

4. Recommendations

Figure 1 illustrates the tasks from Table 1 that are addressed by EAM at each level. As expected, EAM is not a solution to all tasks that arise in the context of the GDPR: we did not find any evidence that EAM contributed to tasks T7 through T9. Nonetheless, we strongly believe that EAM is one key discipline for ensuring GDPR compliance, a view that was shared by most of our interviewees. As I09 said, *"in the end, these data protection topics are connected to the EA elements, regardless of how you define them"*. Another argument for the integration of EA and data protection was presented by I08: *"When the next deadline comes, everybody will start running hectically again, but of course that is not a good approach. I would say it is not a* ***can****, but a* ***must****, it* ***must*** *be integrated with EAM"*.

The feasibility of integrating DPM and EAM, of course, depends on the implementation of the EAM function in the organization. To put this ambition into practice, we give the following recommendations for the respective levels of EAM support:

1. **Advertise EAM as enabler for data protection compliance and foster informal communication between departments**: Some respondents stated that DPM was not aware whether EAM existed and which concerns it addressed in their organization.

2. **Leverage existing information and established tools and processes for data collection**: EAM already has a solid account of applications and processes in the organization, an ideal entry point to identify where personal data is processed. Established tools provide modeling capabilities and support for data collection, and integrating data protection concerns in EAM processes could be more efficient than standalone DPM processes. However, **do not try to document everything in one solution**: Not all information should be represented in EAM. Rather try to identify the shared core concerns and build a community that maintains this information base.

3. **Use EA documentation for analysis of processes and possible threats**: Data flows can support in identifying vulnerabilities and assessing the impact of events like data breaches.

4. **Turn the data protection efforts into an opportunity for digitalization**: Considering necessary standard processes (such as data subject rights or general processing guidelines) early on in software development of acquisition reduces the effort in later stages of the software or business process lifecycle. Knowledge about how personal data is processed is key for optimizing these processes.

5. Discussion and outlook

In this paper, we have given an empirical account of how EAM supported the process of becoming compliant with the GDPR. We interviewed 29 EAM experts in 24 interviews and derived four distinct levels of EAM support for data protection management.

The level of support varies from re-use of EA repositories, mainly application lists (level 1), to active involvement of EA in the data collection efforts (level 2), to support in analyzing the existing landscape for security and data protection risks (level 3), to an active, constructive contribution in defining compliant processes or in aligning business, IT and data protection (level 4). Each of the support levels requires a set of EA artifacts or EAM processes, which are outlined in Figure 1.

We are convinced that EAM can contribute significantly to regulatory compliance, but acknowledge that it is not the one and only solution. Some tasks require more detail than is practical in EA documentation, but EA is in a position to raise awareness for data protection within an organization.

Our results are based on interviews with enterprise architects from German-speaking companies only, and the limited number of interviews does not allow a sound inference of differences with regard to industry or company size. Additionally, we have to remark that the GDPR implementation projects, or the follow-up activities to establish efficient data protection documentation, are still ongoing. Thus, new forms of collaboration between EAM and DPM might evolve.

In the course of this work, we identified a number of possible directions for future research. This work provides an evidence-based description of EA-supported GDPR tasks and focuses rather on the *what* than the *how*. We plan to extend this work by specifying a general process model with roles, tasks and sub-processes for supporting GDPR compliance with EAM.

Our interview guideline covered multiple areas, so we could not cover all aspects that were discussed in the interviews in this work and only shortly touched possible benefits of the collaboration between EAM and DPM in this section. Future work could report on the specific challenges and opportunities that were identified in GDPR implementation projects.

Since we only considered the perspective of enterprise architects in this work, we will elaborate on the perspective of DPM experts in future work. While some interviewees reported reluctant DPM experts, most stated that the EAM support was welcomed by the DPM experts. Informal interviews we held with data protection experts confirmed a rather positive attitude towards the contributions that EAM can make to DPM.

Acknowledgment

This work was sponsored by the German Federal Ministry of Education and Research (BMBF) grant 01IS17049 / UMEDA and the Hamburg Ministry of Science, Research and Equality under the reference LFF-FV 34. The responsibility for the content of this publication lies with the authors.

References

[1] European Union, "Regulation 2016/679 of the European parliament and the Council of the European Union," 2016.

[2] CNIL, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC." https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. Access: 2019-06-14.

[3] TrustArc, "GDPR Compliance Status," tech. rep., 2018.

[4] UK ICO, "Controllers Checklist." https://ico.org.uk/for-organisations/data-protection-self-assessment/controllers-checklist/. Access: 2019-06-14.

[5] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law and Security Review*, vol. 1, 2017.

[6] ISO, IEC, and IEEE, "International Standard ISO/IEC/IEEE 42010:2011 Systems and software engineering Architecture Description," 2011.

[7] P. Aleatrati Khosroshahi, M. Hauder, A. W. Schneider, and F. Matthes, "Enterprise Architecture Management Pattern Catalog v2.0," tech. rep., TU Munich, 2015.

[8] Capgemini, "Digital Architecture Management Study," tech. rep., 2019.

[9] F. Innerhofer-Oberperfler and R. Breu, "Using an Enterprise Architecture for IT Risk Management," in *ISSA*, pp. 1–12, 2006.

[10] E. Grandry, C. Feltus, and E. Dubois, "Conceptual Integration of enterprise architecture management and security risk management," in *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*, pp. 114–123, 2013.

[11] A. Cavoukian and M. Dixon, "Privacy and Security by Design: An Enterprise Architecture Approach September 2013 Information and Privacy Commissioner Ontario, Canada Mark Dixon," 2013.

[12] P. Rozehnal and V. Novak, "The Core of Enterprise Architecture as a Management Tool: GDPR Implementation Case Study," in *26th Interdisciplinary Information Management Talks*, (Kutná Hora, Czech Republic), pp. 359–366, Trauner Verlag, 2018.

[13] F. Burmeister, P. Drews, and I. Schirmer, "A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, pp. 6052–6061, 2019.

[14] L. Sion, P. Dewitte, D. Van Landuyt, K. Wuyts, I. Emanuilov, P. Valcke, and W. Joosen, "An Architectural View for Data Protection by Design," in *IEEE International Conference on Software Architecture, ICSA 2019*, pp. 11–20, 2019.

[15] D. Basin and T. Hildebrandt, "On Purpose and by Necessity : Compliance under the GDPR," *Financial Cryptography and Data Security 2018*, pp. 1–18, 2018.

[16] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation," in *Proceedings - 4th Annual Privacy Forum 2016*, (Cham), pp. 21–37, Springer, 2016.

[17] H. Koç, K. Eckert, and D. Flaig, "Challenging the General Data Protection Regulation (GDPR) with Enterprise Architecture Management (EAM)," *HMD Praxis der Wirtschaftsinformatik*, vol. 55, no. 5, pp. 942–963, 2018.

[18] D. Huth, L. Stojko, and F. Matthes, "A Service Definition for Data Portability," in *21st International Conference on Enterprise Information Systems*, pp. 169–176, 2019.

[19] R. Winter and R. Fischer, "Essential layers, artifacts, and dependencies of enterprise architecture," *Journal of Enterprise Architecture*, no. May, pp. 1–12, 2007.

[20] M. D. Myers and M. Newman, "The qualitative interview in IS research: Examining the craft," *Information and Organization*, vol. 17, no. 1, pp. 2–26, 2007.

[21] J. Saldaña, *The Coding Manual for Qualitative Researchers*. Sage, 2013.

[22] P. Mayring, "Qualitative Content Analysis," *Forum: Qualitative Social Research*, vol. 1, no. 2, pp. 105–114, 2000.

Appendix: Research approach

To collect relevant data, we conducted 24 qualitative interviews with altogether 29 EAM experts, following Myers and Newman [20]. All interview partners currently hold an EAM position or have significant experience through prior EAM positions or executive IT positions. To reduce a possible selection bias, we also encouraged the participation of interview partners who reported little or no EAM contribution to DPM to our initial interview request. The describing details of the interviews are represented in Table 2.

We followed a semi-structured interview guideline, which covered the current role of EA within the company, the employed models and tools, the specific collaboration between EAM and DPM, collaboration with other departments, and possible areas of EAM support for DPM. All interviews were recorded and lasted between 36 and 72 minutes. The recordings were transcribed and yielded a total of more than 100,000 words.

Two researchers analyzed the interview in MAXQDA. We conducted three coding cycles to ensure complete coverage of the material [21] and inductively developed the categories of our codes [22]. The initial codes in the first cycle were based on the interview guide, and were therefore rather coarse: *current EAM practice*, *collaboration with DPM*, *GDPR tasks*, *opportunities*, *barriers*, *EA models*, *EA tools*. In the second cycle, the initial codes were refined into subcodes, for example the specific GDPR tasks that were covered in the interviews. The third cycle comprised a cross-check with other code categories and a reorganization, when necessary.

The conceptual framework was developed in multiple iterations among the researchers and adapted

Table 2. Overview of interviews.

ID	Position	Industry	No. of Employees	Duration
I01	Enterprise Architect	Logistics	5000 - 15000	72 min
I02	Business Architect	Insurance	<5000	62 min
I03	Lead IT Strategy & Architecture	Government	15001 - 50000	61 min
I04	Lead Enterprise Architect	Automotive	>50000	58 min
I05	Lead Enterprise Architect	Professional Services	5000 - 15000	52 min
I06	Enterprise Architect	Insurance	5000 - 15000	57 min
I07	Lead Enterprise Architect	Manufacturing	15001 - 50000	40 min
I08	Enterprise Architect	Insurance	15001 - 50000	43 min
I09	Lead Enterprise Architect	Industrial Services	5000 - 15000	37 min
I10	Enterprise Architect	Insurance	5000 - 15000	48 min
I11	Enterprise Architect	IT Services	<5000	47 min
I12	Enterprise Architect	Consumer Goods	15001 - 50000	65 min
I13	Lead Enterprise Architect	IT Services	15001 - 50000	45 min
I14	Enterprise Architect, Lead Enterprise Architect	Banking	15001 - 50000	60 min
I15	Chief IT Architect	Insurance	<5000	57 min
I16	Enterprise Architect (2)	Automotive	>50000	52 min
I17	Enterprise Architect	Banking	<5000	40 min
I18	Enterprise Architect	Logistics	15001 - 50000	45 min
I19	IT Architect	Banking (CH)	5000 - 15000	53 min
I20	Lead IT Strategy & Architecture	Sports	<5000	65 min
I21	IT Solution Architect	IT Services	>50000	54 min
I22	Enterprise Architect	Automotive	>50000	60 min
I23	Enterprise Architect (4)	Insurance	5000 - 15000	62 min
I24	IT Architect	IT Services	<5000	36 min

iteratively to most accurately represent the results of our interviews. We abstracted and generalized in order to develop a simple, yet descriptive mental model of how EAM supported DPM in the organizations of our interview partners. The recommendations represent a summary of successful practices that were associated with the different levels.