

Empirical Task Analysis of Data Protection Management and Its Collaboration with Enterprise Architecture Management

Dominik Huth^a, Michael Vilser, Gloria Bondel and Florian Matthes

*Chair of Software Engineering for Business Information Systems, Department of Informatics,
Technical University of Munich, Boltzmannstr. 3, Garching, Germany*

Keywords: Data Protection Management, General Data Protection Regulation, GDPR, Enterprise Architecture Management.

Abstract: The General Data Protection Regulation has forced organizations worldwide to rethink their processing activities of personal data. One of the key difficulties of ensuring GDPR compliance is the scope of the regulation and its interdisciplinarity: Data protection management (DPM) has to address challenges on the legal, business and technical level over the entire organization. Enterprise architecture management (EAM) is a well-established discipline that follows a holistic approach to strategically develop the enterprise architecture, consisting of people, processes, applications, and their interrelationships. Thus, DPM can be considered a stakeholder in the EA management process. In this paper, we report on a survey with 38 data protection officers that investigates the main challenges for DPM, as well as the collaboration between DPM and EAM during the implementation of the GDPR.

1 INTRODUCTION

The GDPR has entered into force in 2018, replacing the previous EU directive from 1995 - a time when less than 1% of the world population used internet services (Miniwatts Marketing, 2019). Besides its updated definitions and the extended data subject rights, one of the key changes of the regulation are the dramatic fines (Christina Tikkinen-Piri et al., 2018). Recent announcements by national data protection authorities, e.g. € 50 for Google, GBP 183 million British Airways or GBP 99 million for Marriott (CMS Hasche Sigle, 2019), underline the need to maintain compliance with the regulation.

However, according to a recent industry report, less than half of privacy professionals consider their organization to be “fully compliant” or “very compliant” (Ernst & Young and International Association of Privacy Professionals, 2019). A key problem that is associated with the regulation is its enterprise-wide scope and the interdisciplinarity that this brings with it. While data protection management (DPM) is most frequently conducted by legal functions (International Association of Privacy Professionals, 2019), the GDPR’s accountability principle creates a need to


work more closely with IT and business departments.

Enterprise architecture management (EAM) is a holistic approach to strategically develop and align the technical and business architecture of an enterprise to realize cost saving potentials and increase effectiveness (Farwick et al., 2013). Recent research has stressed its applicability to security and privacy topics as well (Larno et al., 2019; Burmeister et al., 2019).

This work investigates the possible support of EAM for the data protection management tasks. To this end, we define the following research questions:

- **RQ1:** Which DPM activities are necessary to achieve GDPR compliance?
- **RQ2:** What are the most severe problems when conducting these activities?
- **RQ3:** How are DPOs collaborating with EAM and how do they evaluate the helpfulness of EAM?

We first provide an overview about the existing literature that addresses GDPR tasks and concepts describing the interrelationship between GDPR tasks and EAM in section 2. Section 3 describes our research approach and section 4 presents the results obtained from our research. We conclude and point to future areas of work in section 5.

^a  <https://orcid.org/0000-0003-2924-8598>

2 RELATED WORK

2.1 Data Protection Tasks - Academic Contributions

From the academic body of knowledge, we identified a range of analytical and qualitative contributions.

An analytical comparison between the GDPR and the previous Directive 95/46/EC was conducted by (Christina Tikkinen-Piri et al., 2018). Based on the articles of both the directive and regulation, the changes between them are identified and the consequences for organizations processing personal data derived. The authors identify twelve implications for companies that process personal data, of which we consider ten as DPM tasks.

(Sirur et al., 2018) interviewed twelve cyber security experts about the difficulties of implementing the GDPR's requirements. They show that these issues are mainly based on the large scope of the regulation, the enactment of its qualitative recommendations and the necessity of mapping out the organizations' complex data networks.

The work of (Almeida Teixeira et al., 2019) presents a literature review concerning the critical success factors of GDPR implementation. They found out that, among other factors, GDPR analysis, risk identification, process documentation and training awareness are seen as enablers of GDPR implementation. On the other hand, interpretation of the regulation, lack of practical guidelines and standard procedures are some of the barriers identified in their study.

2.2 Data Protection Tasks - Industry Contributions

There exists a substantial amount of industry reports on GDPR implementation, mainly by software vendors or consulting agencies. These reports are often focused on the need to act, with less detailed practical recommendations. We only review a small selection here.

A study that was published shortly before the GDPR entered into force mentions the reengineering of systems and processes as one of the main concerns of respondents (CIPL and AvePoint, 2018). The authors conclude that clarification on how to implement various provisions are needed, among them the conditions for processing, impact assessments and third party processing agreements. According to another global study, less than half of the respondents report being compliant (Ernst & Young and International

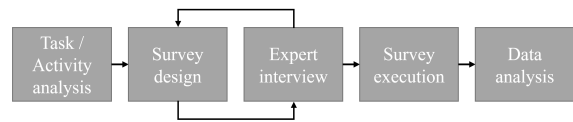


Figure 1: Research Approach.

Association of Privacy Professionals, 2019). As the top responsibilities of DPM, the study cites privacy policies and internal trainings, higher than addressing compliance of single processing activities. In turn, roles outside of the core DPM team are mostly involved in data mapping and addressing processing activities. Recent privacy regulation worldwide seems to support a trend for single global data protection strategies (International Association of Privacy Professionals, 2019). The most frequent operational DPM task from this study are privacy policy changes, followed by privacy impact assessments and records of processing activities. An observation that seems consistent with other studies is the limited occurrence of data subject access requests.

2.3 Collaboration between EAM and DPM

(Burmeister et al., 2019) derive a privacy-driven EA metamodel from an analysis of the GDPR provisions, which represents EA elements and their relationships across six layers. The authors conclude that EA models are useful for achieving compliance with the GDPR and suggest additional research on the integration of EA, privacy and security. One of the DPM tasks that has been addressed in EA research is the record of processing activities (RPA) (Koç et al., 2018; Huth et al., 2019). Other researchers use ArchiMate for modeling security principles, e.g. (Larno et al., 2019).

3 RESEARCH APPROACH

The goal of this study is to derive and validate a set of recurring tasks in DPM on an organizational level. In detail, we aim to rate each task in terms of complexity and time consumption, discover frequently emerging problems and evaluate the status quo of the collaboration between DPM and EAM at this point in time. We illustrate our research process in figure 1:

First we conducted an in-depth analysis of the GDPR, as well as secondary literature from academia and industry that is presented in section 2. The result of this step was an initial list of DPM tasks.

In the second step, we created a questionnaire that consists of four categories:

- Descriptive information about the participant
- The list of tasks, for which we asked the participants to rate their complexity on a five-point Likert scale and to assess their time consumption relative to the participant's total work time
- Problems that arise in the context of addressing the tasks
- The participant's position on collaboration with EAM

We validated and developed our task list and questionnaire iteratively together with four different DPM experts. Three of the experts work as external DPO and one works in DPM in a large organization. We always incorporated the feedback before conducting another interview and did not observe any major changes in the last two iterations.

Fourth, we implemented the questionnaire in the survey tool Questback¹ and distributed the survey in data protection interest groups in professional networks, as well as among personal contacts of the authors.

In the fifth and final step, we visualized and analyzed the survey data. We present the results in the next section.

4 RESULTS

The survey was conducted from August 15th to September 30th of 2019 and resulted in 38 complete responses from data protection officers. 15 of the respondents work as internal DPOs, while the remaining 23 work as external DPOs. When grouping the sample based on the collaboration with EAM, only 12 respondents already collaborate with EAM, leaving 26 DPOs that did not collaborate with EAM at that point in time. Figure 2 shows the (absolute) distribution of participants by company size and the proportions of respondents who collaborate with EAM. The collaboration between DPM and EAM is more pronounced in larger organizations, reflecting the observation that EAM is a discipline that is more prevalent there.

4.1 DPM Activities

As described before, we conducted a literature analysis of primary and secondary sources to identify a valid list of DPM tasks. Choosing the right granularity for these activities poses a challenge, since each of the activities itself consists of multiple steps, which

¹<https://www.questback.com/>

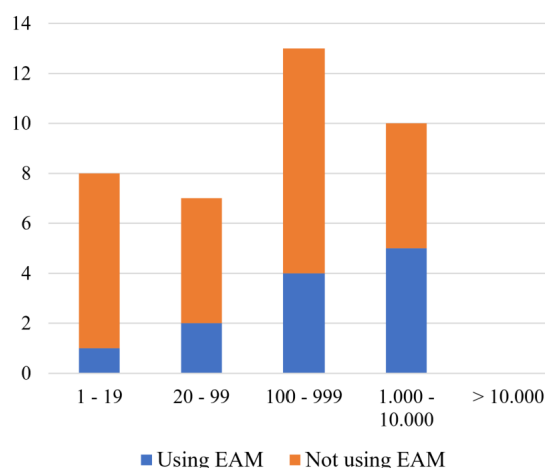


Figure 2: Collaboration with EAM Depending on Company Size (N=38).

are executed by different stakeholders. We opted to define nine activities. Since we evaluated them with four DPM experts we are confident that they represent a valid characterization of data protection management. Further, our questionnaire provided the option of adding further activities. Only one participant used this option to point out certification mechanisms. We argue that these can be included in the verification of compliance and in conducting audits. Our final list of is as follows:

- **Awareness-raising and Schooling within the Organization:** Informing individuals within a company about the GDPR and its implications. It is the responsibility of the DPO to organize training and provide information material to Data Controller, Data Processor and Management.
- **Verifying Compliance of Existing Data Handling Processes:** Processing activities that have already been established before the GDPR might pose a risk for compliance. This also means that if a certain data processing activity is not regulation compliant, measures need to be taken to ensure lawful processing, which is the obligation of the Data Controller. The Data Processor is consulted to actually verify if its provided processing activity is GDPR compliant while the DPO and the Supervisory Authority are only contacted for supporting or clarification purposes.
- **Creation of New Data Handling Processes:** relates to verifying new processing activities that are developed regarding regulation compliance. This activity contains not only setting boundary conditions during the planning phase, for example specifying which kind of data and for what purpose it may be used, but also constantly supervising the

progress of the development. Similar to the prior activity, those tasks often require a thorough understanding of legal obligations imposed by the GDPR. The DPO is usually strongly involved in this activity. In summary, this activity is mainly about applying the data protection by design and by default principle specified in Art. 25 GDPR.

- **Identify Need & Conducting DPIAs:** As described in (Bieker et al., 2016), the data protection impact assessment (DPIA) consists of three stages. In the Preparation stage, it is determined if a DPIA is necessary at all. If that is the case, the scope, involved actors and targets are defined and legal requirements are identified. During the Evaluation stage, the total risk of a processing activity is evaluated. This is done by identifying protection goals, potential attackers and their motives as well as determining evaluation criteria and benchmarks. In the last stage, the Report and Safeguard stage, appropriate safeguards to mitigate the identified risks are selected and implemented. Lastly, a report documenting the evaluation results is created and published, which can then be evaluated by a third party. Once a new processing activity is developed or extended, the process is repeated. For all this, the Data Controller is the responsible actor while relying on the support of the DPO and may consult the Supervisory Authority for clarification purposes.
- **Cooperation with Supervisory Authority:** includes the DPO acting “as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter” as required by Art. 39 GDPR. However, also the Data Controller and Processor are required to cooperate with the Supervisory Authority if necessary (Art. 31 GDPR).
- **Maintaining Records of Processing Activities (RPAs):** Article 30 describes the information that is required in the record of processing activities (RPA), such as the responsible person, the legal basis for processing, or the categories of data subjects and personal data. The DPO supports in compiling the information about all processing activities.
- **Conducting Audits:** Based on a guide published in (UK ICO, 2018), the scope of an audit may cover, inter alia, data protection governance and accountability, data protection training and awareness, and risk management. In summary, an audit is used to verify that all other activities described

in this section are carried out correctly and to discover areas of noncompliance. An audit may be initiated by the Data Controller or by the responsible Supervisory Authority and is performed by the DPO (Art. 28, Art. 39, Art. 58).

- **Dealing with Data Subjects:** Besides reacting to requests based on the Data Subject’s rights (Art. 12 through 22), the communication of a personal data breach to the data subject is also addressed by this activity. The responsible actor thereby is the Data Controller, although usually the DPO acts as the first point of contact, given that his/her contact details normally are publicly available as specified in Art. 37.
- **Report to Management:** is not directly required by the GDPR itself. However, during the expert interviews two interviewees suggested to include reporting to Management as a separate activity. Since it is accountable for the execution of all the activities described above, it is necessary that an organization’s Management is constantly informed about the current situation in DPM.

Note that it is not possible to strictly separate the activities: supporting the creation of processing activities can involve considering a DPIA and preparing information about the processing activity for the RPA. Nonetheless, we consider these tasks to be sufficiently delineated so survey participants could assign them without further explanation.

4.2 Task Complexity & Time Consumption

Figure 3 shows the distribution of responses regarding task complexity, where 1 indicates the lowest level of complexity and 5 indicates the highest level. We arranged the activities in descending order of their average complexity (\bar{x}_c), with “Identify need & conducting DPIAs” being rated as the most complex and “Cooperation with supervisory authority” being rated as the least complex activity. Based on the sample distribution of the five complexity levels for each activity, we assign the activities to three groups:

The first group consists of “Identify need & conducting DPIAs” ($\bar{x}_c = 3.47$), “Verifying already existing data handling processes regarding compliance” ($\bar{x}_c = 3.45$) and “Creation of new data handling processes” ($\bar{x}_c = 3.32$) and can be described as the group of “most complex” activities because of the large amount of participants rating these activities with a complexity level of 4 or 5.

The group of “moderately complex” activities is composed of “Maintaining records of processing ac-

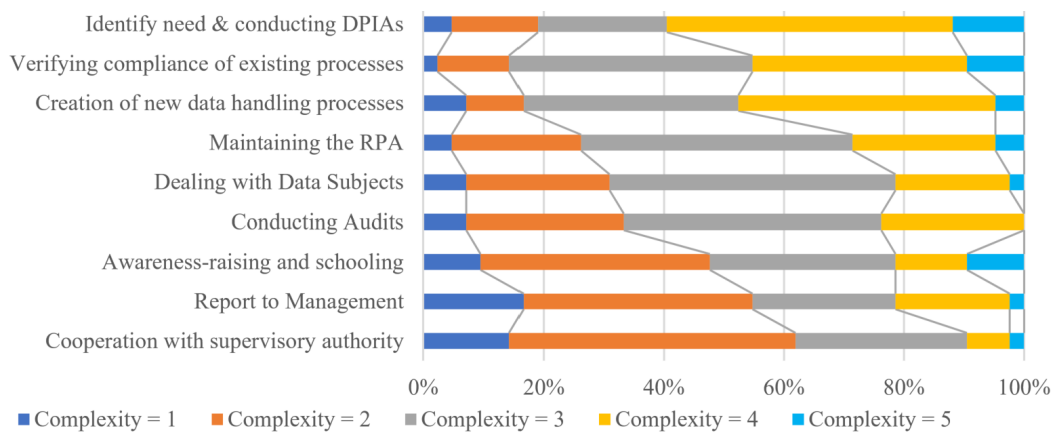


Figure 3: Complexity Distribution of Activities (N=38).

tivities (RPAs)” ($\bar{x}_c = 3.05$), “Dealing with Data Subjects” ($\bar{x}_c = 2.89$) and “Conducting Audits” ($\bar{x}_c = 2.87$), given that complexity level 3 is prevalent here.

Finally, “Awareness-raising and schooling within the organization” ($\bar{x}_c = 2.76$), “Report to Management” ($\bar{x}_c = 2.55$) and “Cooperation with supervisory authority” ($\bar{x}_c = 2.39$) build the group of “least complex” activities, which is based on the high count of complexity level 1 and 2 ratings. Although assigned to the group with the least average complexity, “Awareness-raising and schooling within the organization” was rated as very complex by four participants.

The average time consumption of each activity is shown in figure 4. To prevent a distortion of the results, we decided to exclude the answers of one participant from this examination, given that the time consumption of “Awareness-raising and schooling within the organization” was rated with 100%.

With on average just over 20%, “Verifying already existing data handling processes regarding compliance” was rated as the most time consuming activity by far. While most of the activities consume between 10% to 14% of a DPOs time, “Report to Management”, “Dealing with Data Subjects” and “Cooperation with supervisory authority” were rated as less time intensive.

4.3 Most Frequent Problems

The results of the problem analysis for the whole sample are summarized in Table 5. Per row, the relative frequency of the 38 participants that selected a problem as one of the two most severe ones is shown. Consequently, the upper limit for the sum of each row’s values is 200%. However, it is important to note that the total amount of selected problems differs in some cases significantly from each other. For example, with

an average of 1.7 selected problems per participant, “Verifying already existing data handling processes regarding compliance” shows the highest number of problems of the nine activities. In contrast, usually less than one problem per participant was selected for “Report to Management”, resulting in the lowest number of ticked problems of all activities. For all nine activities on average 1.3 problems were selected. In the following, the characteristics of the problems’ frequency distributions are addressed for each activity.

- For the activity “Awareness-raising and schooling within the organization” especially “Lack of personnel” and “Missing practical guidelines/ standard procedures” often pose a problem.
- When looking at the activities “Verifying already existing data handling processes regarding compliance” and “Creation of new data handling processes”, it is apparent that their frequency distribution of problems is very similar. In both cases, “Lack of personnel” and “Missing practical guidelines/ standard procedures” again are an issue. However, also “Finding the right contact person(s)” and having “Insufficient information on single data processing activities” pose a challenge with almost equal frequency.
- The problems’ frequencies for “Identify need & conducting DPIAs” are quite evenly distributed with around 20% of participants selecting them as most severe. Only the absence of practical guideline and/or standard procedures seems to pose a challenge more often, whereas on the other hand the lack of authority and a holistic view seem like less important problems in that context.
- The “Cooperation with supervisory authority” is mostly hindered because of “Missing practical guidelines/ standard procedures”, “Lack of per-

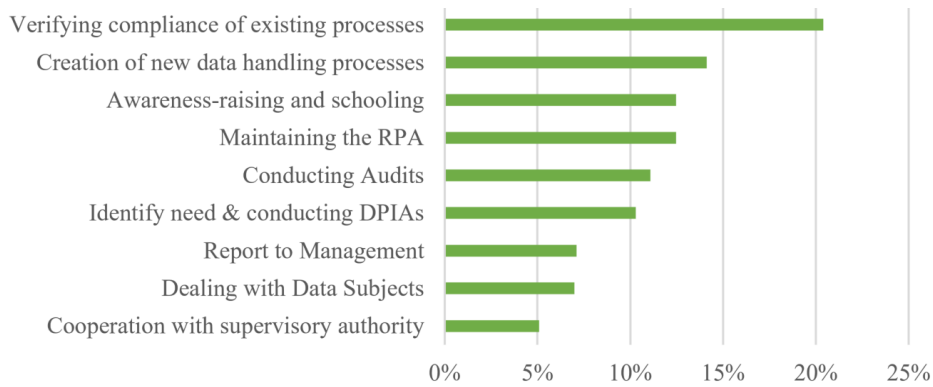


Figure 4: Mean Time Consumption of Activities (N=37).



Figure 5: Frequencies of Problems Rated as Most Severe (N=38).

sonnel” and difficulties with “Finding the right contact person(s)”. The remaining problems thereby only play a subordinate role for most participants.

- For the activity “Maintaining records of processing activities (RPAs)” the problem “Missing practical guidelines/ standard procedures” was selected most frequently by the participants. Although showing lower frequencies, the issues “Missing holistic view on system landscape” and “Insufficient information on single data processing activities” chosen by 21% as well as “Lack of right tools/technology” and “Lack of personnel” selected by 18% of the participants should not be neglected.
- Looking at the activity “Conducting audits”, the issue “Missing practical guidelines/ standard procedures” reaches its highest frequency of all ac-

tivities with 32% of respondents rating it as one of the two most severe ones. However, also a shortage of personnel was reported by 24% of the questioned DPOs.

- When it comes to “Dealing with Data Subjects”, most often “Insufficient information on single data processing activities”, “Inaccuracy of European legislation” and “Lack of right tools/technology” were chosen as most serious issues. The remaining problems were selected equally frequent by 8% of the participants.
- For the last activity, “Report to Management”, the “Lack of Authority” is by far the most severe problem with a selection rate of 26%. Furthermore, a lack of additional personnel was chosen by 16% of the participants. All other problems show a frequency of under 10% in each case.

The problems “Lack of personnel” and “Missing

practical guidelines/ standard procedures” were especially common for most of the activities and were therefore often directly addressed in this section. However, since the frequencies are in general rather evenly distributed, less often selected issues should not be neglected. For example, although the two aforementioned problems show high frequencies in “Awareness-raising and schooling within the organization”, their share of the total number of selected problems for this activity is only 42%.

4.4 Collaboration with EAM

In the last part of the survey, the current status of the collaboration between DPM and EAM was evaluated. The questionnaire was forked to examine the value of EAM support if EAM is already supporting DPM and to discover reasons for a missing collaboration if that is not the case. We therefore use a similar structure for this section by first inspecting the results of the 12 EAM collaborators followed by the reasons for non-collaboration provided by the remaining 26 participants. Finally, the (potential) support of EAM in general is analyzed for both groups.

The participants who are already collaborating with EAM were first asked to rate the support for each of the nine activities. We present the results in figure 6. The activities are presented in decreasing order depending on the average value of EAM support based on the answers for the different levels of helpfulness. For the calculation of the arithmetic mean (\bar{x}_s) the amount of people not using EAM for an activity were therefore excluded. The different levels of helpfulness were weighted as follows: (1) Not very helpful; (2) Somewhat helpful; (3) Very helpful; (4) Extremely helpful. The majority of participants who receive support rated the same as either very or extremely helpful.

For the activities “Verifying already existing data handling processes regarding compliance” ($\bar{x}_s = 2.67$), “Creation of new data handling processes” ($\bar{x}_s = 2.58$), Maintaining records of processing activities” (RPAs) ($\bar{x}_s = 2.58$) and “Identify need & conducting DPIAs” ($\bar{x}_s = 2.33$) each of the 12 participants said they are supported by EAM. Except for DPIAs, the support was rated as very or extremely helpful by at least half of the DPOs. Although the number of EAM supported DPOs decreases for the activities “Awareness-raising and schooling within the organization” ($\bar{x}_s = 2.33$), “Dealing with Data Subjects” ($\bar{x}_s = 2.00$) and “Conducting Audits” ($\bar{x}_s = 1.91$), in the case of the former two activities 75% and in the case of the latter activity 92% of participants still collaborate with EAM. Only the activity “Cooperation with

supervisory authority” ($\bar{x}_s = 1.80$) is usually not supported by EAM and if it is, the value of the support is also rated rather low when compared to other activities.

The 26 participants that stated they are not collaborating with EAM were asked to justify that by providing one or more reasons. Around half of the respondents (n=14) answered that “EAM does not exist in the organization”, by far the most frequently selected reason. Other explanations are “I don’t know if EAM exists in the organization” (n=4) or “Missing contact (persons)” (n=4), followed by “Other goals/objectives/level of detail” (n=3), “No Time/Resources for my part” (n=3) and No Time/Resources on the part of EAM (n=2). Each of the remaining justifications were only selected once. Although the participants were given the opportunity to add their own reasons, only one stated that “The soft- and hardware is provided by an external organization”.

In the last section of the questionnaire the respondents were asked to rate the (potential) support of EAM for DPM, and vice versa, using a 10-point rating scale². As shown in figure 7, the participants who already collaborate with EAM rated the support provided by EAM generally higher than the participants that do not. However, also two respondent who collaborate with EAM evaluate it as “Very low”.

Examining the support of support of DPM for EAM (see figure 8 we see a similar trend. While the distribution of ratings of non-collaborators is almost equal to the one of the general support of EAM for DPM, the DPOs receiving support rate the use of their discipline for EAM lower than the other way around. Nevertheless, collaborators still see a higher value of DPM for EAM than non-collaborators. This time, only one person of the collaborator group rated the support with the lowest possible value.

5 CONCLUSION & OUTLOOK

In this work, we empirically evaluated DPM tasks with respect to their complexity, the time consumption and the main problems that occur when conducting these activities. We did this with literature analysis, four qualitative expert interviews and a quantitative survey with 38 DPOs. Additionally, we evaluated the current or potential future support with EAM from the DPO’s perspective. Thus, our three research questions can be answered:

²Due to the different sample sizes (12 to 26), we use relative frequencies in figures 7 and 8.

Usefulness of EAM

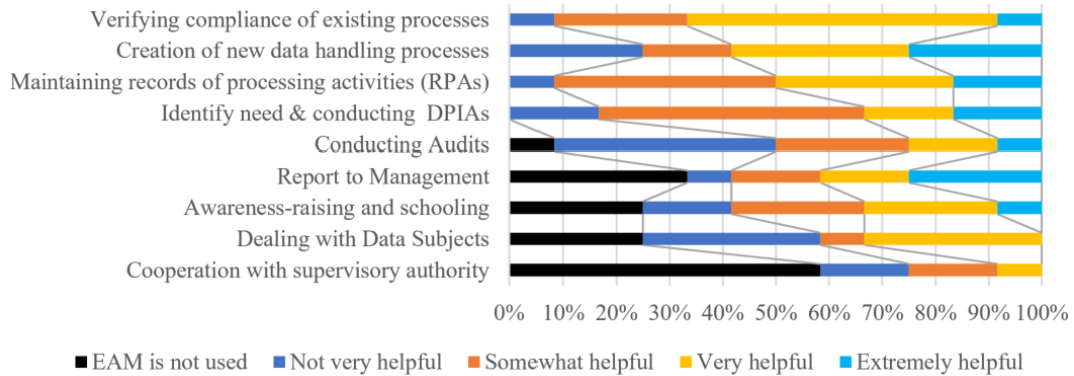


Figure 6: Distribution of EAM Support Effectiveness (N=12).

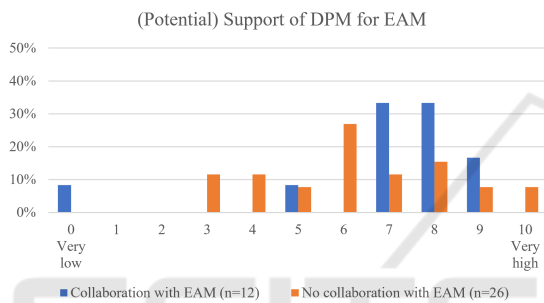


Figure 7: (Potential) Support of EAM for DPM (N=38).

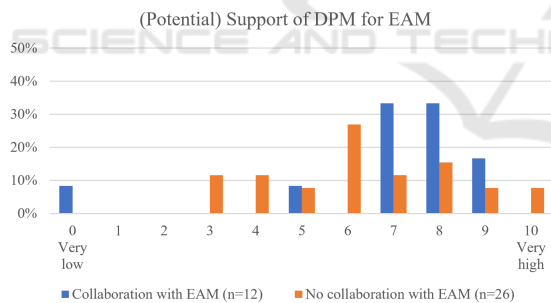


Figure 8: (Potential) Support of DPM for EAM (N=38).

RQ1: Which DPM Activities are Necessary to Achieve GDPR Compliance?

Based on related work and the input of four DPM experts, the spectrum of tasks in DPM was grouped into nine activities which were rated in terms of complexity and time consumption by the survey participants. Based on the distribution of rated complexity levels, each activity could be assigned to a group of either *rather complex*, *moderately complex* or *rather easy* activities. For an activity’s time consumption its relative average share of a DPOs total work time is used as a measure. In the following, the final list of ac-

tivities with their respective rating in complexity and time consumption (TC) is presented:

Most Complex:

- Identify need & conducting DPIAs (TC ≈ 10%)
- Verifying already existing data handling processes regarding compliance (TC ≈ 20%)
- Creation of new data handling processes (TC ≈ 14%)

Moderately Complex:

- Maintaining records of processing activities (RPAs) (TC ≈ 13%)
- Dealing with Data Subjects (TC ≈ 7%)
- Conducting Audits (TC ≈ 11%)

Least Complex:

- Awareness-raising and schooling within the organization (TC ≈ 13%)
- Report to Management (TC ≈ 7%)
- Cooperation with supervisory authority (TC ≈ 5%)

Given that the nine activities were selected and evaluated during the four expert interviews and subsequently verified by 38 DPOs during the questionnaire, it can be said with confidence that these activities may be used to reliably cover the range of tasks in DPM. Furthermore, the activities’ complexity and time consumption characteristics may be used to determine the activities where support is most urgently needed. Following this line of thought, especially the activities “Verifying already existing data handling processes regarding compliance” and “Creation of new data handling processes” should be considered first when designing support measures, which in turn may focus on mitigating the respective problems for these activities.

RQ2: What are the Most Severe Problems when Conducting these Activities?

In the second part of the survey, the participants were asked to rate the two (or less) most severe problems for every activity. As we show in figure 5, the frequencies of the different problems vary considerably depending on the underlying activity. Nonetheless, we found that a lack of personnel is for many activities one of the most severe issues which might be rooted in organizations seeing GDPR compliance more as a hindrance that must be overcome with as little resources as possible, instead of viewing it as an opportunity for achieving a competitive advantage (Almeida Teixeira et al., 2019). Furthermore, implementing guidelines or standard procedures may be supported by an integrated tool support approach and might reduce the effort of performing certain activities. An official guide or self assessment as provided in (UK ICO, 2018) may therefore be integrated in DPM and should at the same time reduce the ambiguity of the legislation. Finally, we showed that for process-heavy activities there is often a lack of detailed information about a single data handling process as well as missing contact persons. A stronger focus on documentation (for future verification purposes) as well as using other information sources (for current verification purposes), such as the EA, may therefore be necessary to effectively mitigate these problems.

RQ3: How are DPOs Collaborating with EAM and How do they Evaluate the Helpfulness of EAM?

From the 38 participants, only 12 stated they collaborate with EAM. The most often provided reason for this low collaboration rate is by far the nonexistence of EAM in the organizations. While the group of non-collaborators is rather indecisive in their attitude towards a collaboration with EAM, the DPOs that do work together with EAM consider the collaboration significantly more helpful. Furthermore, in both groups the (potential) support of EAM for DPM was rated higher than the support of DPM for EAM. When looking at the EAM support for the nine activities, it can in general be described as quite effective. It proves especially helpful for reporting to management and verifying already existing data handling processes as well as for the creation of new data handling processes and maintaining RPAs. Only the cooperation with the supervisory authority is rather ineffectively supported if it is at all.

Outlook

Our findings validate future research that addresses one or more DPM activities. With respect to the collaboration between EAM and DPM, future research might detail on organizational factors that influence this collaboration, e.g. maturity levels of EAM. Our future work aims at advancing the notions of privacy and data protection from the perspective of EAM.

ACKNOWLEDGEMENTS

This work was sponsored by the German Federal Ministry of Education and Research (BMBF) grant 01IS17049 / UMEDA and X-DACE. The responsibility for the content of this publication lies with the authors.

REFERENCES

- Almeida Teixeira, G., Mira da Silva, M., and Pereira, R. (2019). The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 25(4):1.
- Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., and Rost, M. (2016). A process for data protection impact assessment under the european general data protection regulation. In Schiffner, S., Serna, J., Ikonoum, D., and Rannenber, K., editors, *Privacy Technologies and Policy*, pages 21–37, Cham. Springer International Publishing.
- Burmeister, F., Drews, P., and Schirmer, I. (2019). A privacy-driven enterprise architecture meta-model for supporting compliance with the general data protection regulation. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.
- Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula (2018). Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153.
- CIPL and AvePoint (2018). Organisational Readiness for the European Union General Data Protection Regulation. Technical report.
- CMS Hasche Sigle (2019). GDPR Enforcement Tracker. <http://www.enforcementtracker.com/>, accessed 2019-11-29.
- Ernst & Young and International Association of Privacy Professionals (2019). IAPP-EY annual privacy governance report 2019. Technical report.
- Farwick, M., Breu, R., Hauder, M., Roth, S., and Matthes, F. (2013). Enterprise architecture documentation: Empirical analysis of information sources for automation. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, pages 3868–3877.

- Huth, D., Tanakol, A., and Matthes, F. (2019). Using Enterprise Architecture Models for Creating the Record of Processing Activities (Art . 30 GDPR). In *23rd IEEE International Distributed Object Computing Conference (EDOC)*, Paris.
- International Association of Privacy Professionals (2019). Measuring Privacy Operations. Technical report.
- Koç, H., Eckert, K., and Flaig, D. (2018). Datenschutzgrundverordnung (dsgvo): Bewältigung der herausforderungen mit unternehmensarchitekturmanagement (eam). *HMD Praxis der Wirtschaftsinformatik*, 55(5):942–963.
- Larno, S., Seppänen, V., and Nurmi, J. (2019). Method Framework for Developing Enterprise Architecture Security Principles. *Complex Systems Informatics and Modeling Quarterly (CSIMQ)*, 117(20):57–71.
- Miniwatts Marketing (2019). Internet World Stats. <https://internetworldstats.com/stats.htm>, accessed 2019-10-01.
- Sirur, S., Nurse, J. R. C., and Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, pages 88–95. ACM.
- UK ICO (2018). A guide to ICO audits. <https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf>, accessed 2019-11-28.

