H. Roßnagel et al. (Eds.): Open Identity Summit 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 177

Enabling SMEs to comply with the complex new EU data protection regulation

Nicolas Fähnrich[1], Michael Kubach[1]

Abstract: The European General Data Protection Regulation (GDPR) introduces privacy requirements that pose a complex challenge especially for small and medium sized enterprises (SMEs). In this paper, we present a software-supported process model developed by us that helps SMEs to establish processes ensuring the rights of the data subjects and prepare the documentation that is necessary to comply with the GDPR. Three small case studies illustrate the work with the process model and lessons learned from these practical applications of our tool give further insights into the topic.

Keywords: GDPR; case study; process model; privacy; data protection; compliance; SME

1 Introduction

The trend to digitize business processes and the networking of production and supply chains is leading - whether intentionally or unintentionally - to a sharp increase in the volume of personal data collected. Legislators reacted with new regulations for data protection and data security [KGH16]. On May 25th 2018, the European General Data Protection Regulation (GDPR) [Eu18] went into full effect and is having an extensive impact on the handling of personal data, and thereby challenging European companies. The documentation duties required when processing personal data were massively extended and, among other things, customers and employees receive far-reaching rights regarding transparency, correction and deletion of personal data. Compared to the previous legislation, companies that violate these laws risk significantly increased fines up to 20 million Euros or 4 percent of the worldwide annual turnover of the parent company [TPRM18]. Based on our experience in consulting companies regarding IT-security and privacy matters, particularly small and medium sized enterprises (SMEs) face serious difficulties in meeting the requirements of the GDPR. These companies usually lack processes regarding privacy, quality management and IT-security. This makes it difficult for them to identify the protection needs and the necessary security measures to meet the goals of the GDPR. Thus, SMEs need support dealing with the regulation through a systematic approach with practical tasks for the companies. Proposed models that are supposed to prepare companies for the GDPR [Bi16] [Fr16] [Wy16] often cover only parts of the regulation, come from a legal perspective, are either very complex or superficial and therefore not practical for SMEs. The lack of support

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

for companies in implementing the GDPR could be seen as one important factor for the insufficient number of companies that have done so. A recent report by the German industry association Bitkom states that three out of four companies have failed to implement the GDPR by May 25th and many still haven't finished the process [Bi18]. This paper, thus, presents a software-supported process model that addresses the challenges the GDPR poses especially to SMEs and enables an efficient approach for them to comply with the regulation.

2 Process model

As already argued in the introduction, the GDPR introduces complex requirements for companies. A central component to meet these requirements is the necessity to be able to analyze all business processes individually including all personal data that is processed. To structure those requirements and lead the companies step-by-step through the necessary tasks required to meet them we have developed a process model. The model includes nine process steps, structured into two main parts, and is explained below in detail.

The part "description of the overall system" includes step 1, the complete inventory of the infrastructure. This comprises of a full documentation of all IT-systems or analog systems (dealing with information) that are used by the enterprise considered. Step 2 is a complete documentation of all business processes with a clear mapping of all involved infrastructure components that were documented in step 1. The description of the business processes includes a complete list of all categories of personal data that are processed. These steps deliver the first results, a complete description of all systems and processes and are critical for the quality of the analysis and the end result. Critical personal data that is left out can lead to a massive misjudgment of required data protection in the subsequent steps. The second part of the process model "data protection / risk analysis" starts with step 3, the identification of protection needs. Regarding the documented categories of personal data in step 2, possible damage scenarios are identified and the possible impact for the persons affected is estimated. Thereby the maximum extent of the damage determines the protection needs. Considered are damages to the social position, economic conditions or the health of the affected people. In order to ensure a complete analysis of possible damage scenarios, 6 protection goals (the protection goals are an extension of the CIA-triad, which represents basic information security goals) are defined and analyzed individually: Confidentiality, integrity, availability, unlinkability, transparency and intervenability [He11]. Once the protection needs have been determined for all business processes, these are transferred to the related infrastructure components. The protection needs of these are again determined using three factors. First, the maximum protection required by the assigned business processes. Second, the distribution effect (d): A high number of infrastructure components (c) that are used in a single business process (p) can justify a lower classification of the protection need of the considered component, if it only plays an insignificant role for the process and the related data. Its indicator is defined as: $d(p_i) = 1/\sum_{j=0}^{n} c_{ij}$. Third, the cumulative effect (k): A high number of processes in which a single infrastructure component is involved

can justify a higher classification of the protection needs of the considered component. Its indicator is defined as: $k(c_i) = 1/\sum_{j=0}^{n} p_{ij}$. In step 4, possible hazards to the infrastructure are identified and rated based on their probability of occurrence. This is done individually for each infrastructure component. The identification of hazards is done by matching with a catalog (based on existing catalogs like the German "IT-Grundschutz") that was created for this process model. With the results from steps 3 and 4 the risks for the infrastructure components and the associated business processes is determined using the matrix shown in Figure 1 (step 5). In the following step 6, appropriate technical and organizational measures

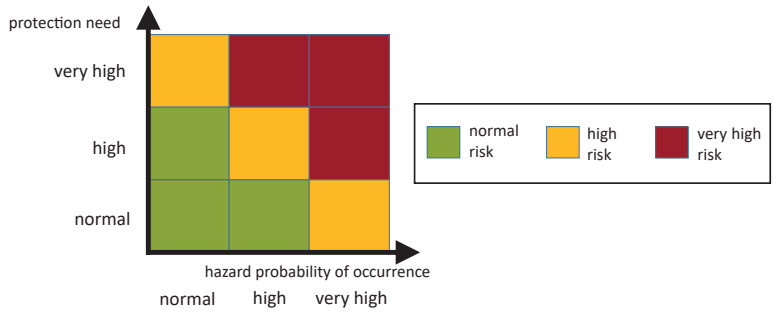

Fig. 1: Risk matrix

are chosen to address the determined risks. In the next 2 steps, these are compared with the measures already implemented as part of a gap analysis. The final step completes the process model and results in an GDPR report. The description of the overall system can be very challenging, especially when there is no preliminary work such as a list of all business processes or of the IT-systems. The process model was designed to meet the requirements of the GDPR independently of existing work and without the need for additional methods or tools. To facilitate the application of the process model and increase its efficiency we have developed a software that supports the user in all steps of the process. As part of the documentation, the explicit assignment of infrastructure components to business processes is partially automated. This approach ensures that the logic link between the infrastructure and the procedures is guaranteed. The software automatically calculates the required indicators to determine the protection needs for every infrastructure/business process combination and assists the user in all further steps. The case studies illustrate the need for such a software assistance.

3 Three small case studies

The process model has already been used in several projects. In the following, we present three case studies that have helped us to evaluate the tool for practical viability and gave implications for its further development. Moreover, they give a glimpse into the state of IT-security and privacy in German SMEs. After a brief description of the companies, the initial situation is described, followed by the results of steps 1 to 5 of the process model.

3.1 Case study 1: SME in the chemical sector

The company located in southern Germany employs fewer than 10 persons and offers services in the chemical branch (industrial). The customers are almost exclusively within the business-to-business sector. The initial situation revealed serious shortcomings in meeting the requirements of the GDPR. Apart of a listing of business processes, no IT-security or privacy protection analysis, such as a privacy and data protection impact assessment were conducted prior the application of our process model. Neither a procedure to inform concerned persons about the collection of personal data, nor a procedure to report data breaches are implemented. The company's infrastructure comprises 12 different

Inf. comp.	**Protection need**			**Vulnerability**			**Risk**		
	CS1	CS2	CS3	CS1	CS2	CS3	CS1	CS2	CS3
1	Normal	High	High	Normal	High	High	Normal	High	High
2	Normal	High	High	Normal	High	High	Normal	High	High
3	High	High	High	High	High	Normal	High	High	Normal
4	Normal	High	High	High	Normal	Normal	Normal	Normal	Normal
5	Normal	High	High	Normal	Normal	Normal	Normal	Normal	Normal
6	Normal	Normal	High	Normal	Normal	Normal	Normal	Normal	Normal
7	Normal	High	High	Normal	Normal	Normal	Normal	Normal	Normal
8	High	High	High	High	Normal	Normal	High	Normal	Normal
9	High		High	Normal		Normal	Normal		Normal
10	High		High	High		Normal	High		Normal
11	High		High	Normal		Normal	Normal		Normal

Tab. 1: Risk analysis of the three case studies (CS1, CS2, CS3)

components[2]. Matching these with 6 documented business processes reduces the number of infrastructure components to be considered to 11 and results in 22 combinations of business processes and infrastructure components. The protection need of each business process in every combination as well as the distribution effect and the cumulative effect is taken into account and results in 6 components with normal protection needs and 5 components with high protection needs. The corresponding indicators d and k that have been defined in the previous section are calculated automatically for every combination by our software supported process model. On a scale of 1 (normal protection need) to 3 (very high protection need), the average protection need amounts to $p = 1.45$. As part of the risk analysis 135 hazards were identified with an average probability of occurrence of 1.33 (based on a scale of 1 [low] to 3 [high]). The identified hazards were condensed to a vulnerability for every infrastructure component considering the average and the maximum probability of occurrence, which leads to the results shown in Table 1 (CS1 for Case study 1). For 3 infrastructure components, a high risk was identified, whereas the other components show a normal risk. This results in an average risk of $r = 1.27$. Based on these results, appropriate technical and organizational measures were taken to address the risk.

[2] Infrastructure components: IT-systems, data storage media (analog/digital). In the summation of components multiple identical components are aggregated (e.g. 10 Windows clients equal 1 component)

3.2 Case study 2: SME in the printing sector

The small company located in southern Germany has less than 10 employees and is active in the printing sector. The customers are enterprises of different sizes, up to big multinational corporations. The initial situation is comparable to case study 1. There was no directory of business processes, no listing of IT-systems in use, neither a previously conducted IT-security or privacy protection analysis, nor a procedure to inform concerned persons about the collection of personal data or a procedure to report data breaches. In fact, we learned when conducting our analysis that security standards were pretty low. Computers were virtually always on and screens never locked. The server room was always open and the server had already been taken over by criminals once and used to send out SPAM. No significant consequences had been drawn from this incident and the company kept it secret in fear to scare off customers. The infrastructure totals 10 components, 8 of which are used in 3 documented business processes. Our matching process yields 12 combinations of infrastructure components and business processes. Applying the same process steps described in the previous case study, 7 infrastructure components with a high protection need and 1 component with a normal protection need were identified, resulting in an average protection need of $p = 1.87$. As part of the risk analysis, 100 hazards with an average probability of occurrence of 1.2 were identified leading to the results presented in Table **??** (CS2). The analysis results in 3 components with a high and 5 components with a normal risk. Although the average protection need is fairly high, the average risk is $r = 1.2$.

3.3 Case study 3: SME in the medical sector

In the third case study, we had a look at a small company in the medical sector that has 8 employees. The company is located in southern Germany. In contrast to case studies 1 and 2, in this case the majority of customers are end customers, which, combined with critical personal data categories, leads to a high protection need in many business processes. The initial situation showed similarly serious deficiencies with regard to the requirements of the GDPR as before. No directory regarding the business processes and the IT-infrastructure was in place. There was no preparatory work on protection needs and risk analyses, nor were procedures to inform concerned persons about the collection of personal data or report data breaches in place. With 13 infrastructure components, 11 of which are relevant for the analysis, and 7 documented business process our matching yields 36 combinations of infrastructure components and business processes that were analyzed further. This analysis resulted in a high protection need for every business process ($p = 2.0$). The risk analysis identified 113 hazards for the infrastructure with an average probability of occurrence of 1.16. Table **??** (CS3) shows the results. The analysis yields 2 components with a high and 9 components with a normal risk, resulting in an average of $r = 1.2$.

3.4 Lessons learned from the case studies

At least in Germany many requirements of the GDPR like a complete directory of business processes and IT-systems are not new. Companies that have previously complied with the data protection and privacy legislation are unlikely to spend much effort meeting the new requirements, however if little or no preliminary work exists, the effort can be very large depending on the complexity of the company. Therefore, it was a bit surprising to learn in our case studies that many companies do not meet these requirements at all. To determine

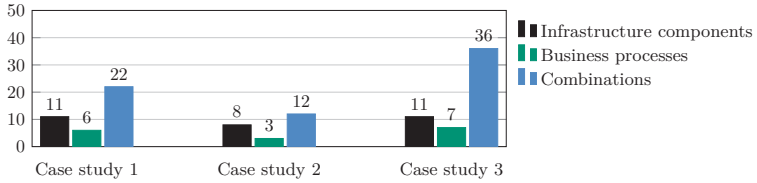

Fig. 2: Number of infrastructure components and business processes

the risk for every infrastructure component, the vulnerability of the component and the need for protection of every business process in which the component is used have to be taken into account. Depending on the number of infrastructure components and business process, the number of combinations can be very large as shown in Figure 2. We found that even in small companies, the complexity is quite large. By using our software supported process model, the possible combinations are automatically matched and evaluated, thus minimizing the required effort. This shows that even in small companies this task needs to be automated. We have seen that even with a high protection need, the actual risk can be significantly lower (case study 3: average protection need of $p = 2.0$, average risk of $r = 1.2$). This shows that a holistic risk assessment of processed personal data requires a complete analysis of both, the processes and the infrastructure. Other approaches, solely based on estimations, do not provide sufficient validity and may lead to the selection of insufficient or excessive technical and organizational security measures.

4 Conclusion

The data protection requirements of the GDPR exceed previous regulations and provide a huge challenge for companies of any size. SMEs in particular lack resources to approach these challenges and are usually ill-prepared for the measures that need to be taken. We have therefore developed the process model described in this paper. Our process model has already been applied successfully in several consulting projects, three of which were presented as case studies. In all case studies, the requirements of the GDPR were not fulfilled in the initial situation. Actually, security and privacy standards in the majority of cases were alarmingly low. The studies further showed that the complexity of the overall system of business processes, infrastructure components and categories of personal data processed is often very large, even in small companies. Especially regarding this problem,

our software-supported process model ensures high efficiency through automation. We have shown that the determined protection needs of the infrastructure components do not correlate directly with the derived risks and that an analysis of the infrastructure and the business processes is required to determine the risks. Of course, the extent of insight from just three case studies is limited. We cover only certain industry sectors and all companies in our study handle just a limited amount of personal data. Moreover, only time can tell if the companies really implement the measures and processes suggested by our model and keep them updated. Therefore, we follow the development and consider an extended case study analysis in the future. Nevertheless, we think that our model has already proven that it is suited for practical application. As our three cases have shown, the protection level of personal data and the IT-security in SMEs is often very low and can be raised significantly through our tool. Therefore, we keep working with it, the feedback from the companies is positive and we continually adjust it based on our lessons learned. For our work it is a viable tool that is applicable for SMEs especially regarding their limited resources. It helps SMEs to cope with the complex requirements of the GDPR and avoid its drastic fines. Perhaps most importantly, our process model makes them capable to protect the personal data of employees and customers, as it was the original intention of the regulation.

Bibliography

[Bi16] Bieker, F.; Friedewald, M.; Hansen, M.; Obersteller, H.; Rost, M.: A process for data protection impact assessment under the european general data protection regulation. In: Annual Privacy Forum. Springer, pp. 21–37, 2016.

[Bi18] Bitkom: Umsetzung der Datenschutzregeln an vielen Stellen weiterhin unklar. 2018.

[Eu18] European Parliament and Council: , Regulation (EU) 2016/679 (General Data Protection Regulation), 2018.

[Fr16] Friedewald, M.; Obersteller, H.; Nebel, M.; Bieker, F.; Rost, M.: White Paper Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz, 2, 2016.

[He11] Hedbom, H.; Schallaböck, J.; Wenning, R.; Hansen, M.: Contributions to standardisation. In: Privacy and Identity Management for Life, pp. 479–492. Springer, 2011.

[KGH16] Kubach, M.; Görwitz, C.; Hornung, G.: Non-technical Challenges of Building Ecosystems for Trustable Smart Assistants in the Internet of Things: A Socioeconomic and Legal Perspective. In (Hühnlein, D.; Roßnagel, H.; Schunck, C.; Talamo, M., eds): Open Identity Summit 2016, Lecture Notes in Informatics – Proceedings, pp. 105–116. Köllen, Bonn, 2016.

[TPRM18] Tikkinen-Piri, C.; Rohunen, A.; Markkula, J.: EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1):134–153, 2018.

[Wy16] Wybitul, T.: EU-Datenschutz-Grundverordnung im Unternehmen: Praxisleitfaden. Fachmedien Recht und Wirtschaft, 2016.