A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria

Sandra Domenique Zinsmaier[1,2,4] [a], Hanno Langweg[2,3] [b] and Marcel Waldvogel[4] [c]

[1] *Siemens Logistics GmbH, Konstanz, Germany*

[2] *HTWG Konstanz University of Applied Sciences, Konstanz, Germany*

[3] *Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU, Norwegian University of Science and Technology, Gjøvik, Norway*

[4] *University of Konstanz, Konstanz, Germany*

Keywords: Common Criteria, GDPR, Privacy by Design, Requirements Engineering, Security by Design.

Abstract: We propose and apply a requirements engineering approach that focuses on security and privacy properties and takes into account various stakeholder interests. The proposed methodology facilitates the integration of security and privacy by design into the requirements engineering process. Thus, specific, detailed security and privacy requirements can be implemented from the very beginning of a software project. The method is applied to an exemplary application scenario in the logistics industry. The approach includes the application of threat and risk rating methodologies, a technique to derive technical requirements from legal texts, as well as a matching process to avoid duplication and accumulate all essential requirements.

1 INTRODUCTION

Requirements engineering is a fundamental procedure in every software development lifecycle. Nowadays, it is essential to develop software products that consider security and privacy by design from the very beginning. Therefore, there exists a need for specific, detailed security and privacy requirements that also ensure legally compliant software. This is not holistically considered by classical requirements engineering techniques. Therefore, we developed an approach that provides a structured way to identify requirements from various stakeholders, match related requirements to avoid duplication and track requirements for compliance assertion.

Certifications like *ISO 27001* or *Common Criteria* (CC) are required by customers more often such that vendors of software products have to consider getting their products or organization certified. According to Art. 24(3) of the General Data Protection Regulation (GDPR), compliance with a code of conduct or certification may be used to prove lawfulness to certain articles of the GDPR. Thus, it is interesting to find the delta between requirements from the various stakeholders and accumulate all necessary requirements in the very beginning of the software project.

The proposed approach assembles requirements that emerge from various stakeholders, e.g., vendor, customer, government, as well as requirements from an aspired CC evaluation (by evaluating CC security functional requirements (SFRs) that are described in CC Part 2 (Common Criteria, 2017)). We apply the methodology to a practical scenario in the logistics industry. As a result, we present a list of detailed requirements that – once implemented – make the exemplary software product compliant with the GDPR and partially prepared for a CC evaluation.

The remainder of this paper is structured as follows. Section 2 provides an overview of related research. Then, the application scenario and methodology are described in sections 3 and 4. The method is applied to the exemplary application scenario in section 5. We conclude with a discussion in section 6.

2 RELATED WORK

We elaborate on three interconnected areas of work in the context of requirements engineering: GDPR compliance, threat and risk assessment, as well as Common Criteria.

In (Palmirani et al., 2018; Bartolini et al., 2018b), a model for legal reasoning and compliance with re-

[a] https://orcid.org/0000-0002-3811-6151

[b] https://orcid.org/0000-0002-4156-5775

[c] https://orcid.org/0000-0003-1665-0166

Zinsmaier, S., Langweg, H. and Waldvogel, M.
A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria.
DOI: 10.5220/0008960604730480
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 473-480
ISBN: 978-989-758-399-5; ISSN: 2184-4356

gard to the GDPR is proposed using logic formulæ. This model is validated in (Bartolini et al., 2018a) on Art. 5(1)(a) and Art. 7(1) GDPR using the methodology proposed in (Bartolini et al., 2018b). While this approach provides a formalization of GDPR articles in a human-readable format that could then be used to validate compliance to the law, it still lacks bridging the gap between legal requirements and technical requirements.

The work by (Pandit et al., 2018b) utilizes the GDPRov ontology developed in (Pandit and Lewis, 2017) along with the GDPRtEXT resource presented in (Pandit et al., 2018a) in order to provide a way to represent and query GDPR compliance obligations. Again, the approach lacks referring to specific technical requirements based on the identified legal requirements.

A methodology for auditing GDPR compliance is proposed by (Basin et al., 2018). Their inter-process data-flow model includes the formal notion of business process modelling for identifying and implementing the purpose for data processing as well as automated algorithmic verification of GDPR compliance which may be complemented by human interactions. The work focuses only on the following concepts of the GDPR: purpose limitation, data minimisation, consent and the right to be forgotten.

How ISO 27001 can help to achieve GDPR compliance is described in (Lopes et al., 2019). While many useful parallels are shown and best practices from ISO 27001 provide useful technical details for complying to certain GDPR requirements, it is concluded that conforming to ISO 27001 does not guarantee GDPR compliance; however, it facilitates certain aspects.

An IoT healthcare system is taken as application scenario in order to design a GDPR compliant system by (Kammüller, 2018; Kammüller et al., 2019). However, compliance of the system is not traceable as there are no references to corresponding GDPR Articles.

In the context of data protection by design, the research by (Dewitte et al., 2019) shows that there is a discrepancy in risk assessment between legal experts (making data protection impact assessment) and software engineers (doing threat modeling). Requirements are defined and categorized as legal description requirements or architectural description requirements. They show which state-of-the-art threat modeling techniques fulfill which legal and architectural requirements in order to do a comprehensive risk assessment. As a result, none of the methodologies support all requirements in both categories – legal and architectural. Instead, most categories fulfill either legal or architectural requirements. Thus, previous work (Ringmann and Langweg, 2017) first conducted the risk assessment using STRIDE, resulting in an initial set of architectural requirements. These requirements are expanded and matched by technical requirements which were derived from legal requirements in (Ringmann et al., 2018).

To the dichotomy between data protection impact assessments and threat modeling with the focus on privacy by design refers (Sion et al., 2019). Their approach provides a meta-model for a data protection architectural viewpoint using data flow diagrams and including the reference to requirements imposed by the GDPR (e.g., data-minimization, purpose limitation). However, the approach lacks security-related requirements with regard to the GDPR. A summary of related research bridging the gap between legal and computer science approaches to privacy is provided by (Nissim et al., 2018).

(Jensen et al., 2019) propose a research agenda regarding the alignment of software development with GDPR requirements. A summary of related research regarding bridging the gap between legal and computer science approaches to privacy is provided by (Nissim et al., 2018).

The work by (Yin and Qiu, 2010) bridges the gap between CC security functional requirements (SFR) and traditional requirements description language by proposing a three stages security requirements development model. In (Amara et al., 2019), security requirements are defined from CC for software development and applied in a case study.

Another approach to bridge the gap between abstract legal requirements and concrete technical requirements is presented by (Bräunlich et al., 2011; Simić-Draws et al., 2013) through the application of the method KORA in combination with Common Criteria. KORA is the abbreviation for "Konkretisierung rechtlicher Anforderungen" (concretization of legal requirements) which was introduced by (Hammer et al., 1992) and has been used in German legal research. The work by (Bräunlich et al., 2011) combines the application of CC with KORA in the application context of ballot secrecy. In continuation, (Simić-Draws et al., 2013) presents a framework that integrates KORA in the context of CC and ISO 27001. The framework is then also applied to a ballot secrecy scenario. In (Simić-Draws et al., 2013), the process steps of CC and ISO 27001 are matched to the four process steps in KORA. Previous work (Ringmann et al., 2018) applied KORA to the GDPR and identified 74 generic, reusable technical requirements that can be applied to software products which process personal data.

3 APPLICATION SCENARIO

For the example application, we choose a scenario within the logistics domain that is presented in (Ringmann and Langweg, 2017). In order to deliver items from one location to another, it is necessary to identify the destination information which is placed upon the item in writing. This information can be present in various forms, e.g., handwriting, typewriting, bar code, on a form, or an address label. As a result, personal data that is processed usually includes a person's postal address and name. The process between posting an item for sending and final delivery of the item to the destination location includes one or multiple sorting stages where items with similar destinations are assembled. At each sorting stage, a machine determines the destination information of an item by scanning the item with cameras, extracting the location of an address through highly specialized optical character recognition (OCR) software and then routing the item to a delivery vehicle for further/final distribution. This process is similar for correctly sorting and processing mail, packages as well as baggage items.

While the sorting machine does the physical routing, the information processing is done on a computer where OCR algorithms extract address information from the scanned image. Identified destination addresses are then compared to corresponding entries in a data dictionary and, eventually, identified address data is sent back to the sorting machine as a structured dataset that contains the destination information. This simplified process is displayed in Fig. 1. For the remainder of this paper, we work with the following components of the sorting process:

- Scans of personal data: images from the scanner, interface to the scanner
- Data dictionary (DB): database of addresses/routing information, interface from the software to the data dictionary
- Software/Algorithms: software solution, also including physical hardware
- Identified personal data: structured dataset containing routing information, interface to sorting machine

4 METHOD

The proposed methodology leverages upon (Ringmann and Langweg, 2017; Ringmann et al., 2018).

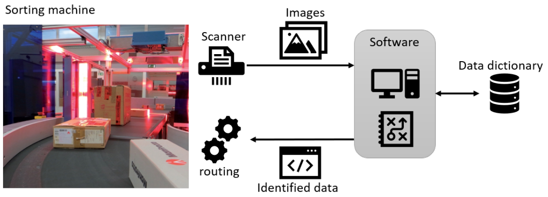

Figure 1: Simplified sorting process.

First, main stakeholder interests and threat scenarios for the proposed application scenario are identified in (Ringmann and Langweg, 2017) utilizing the STRIDE methodology (Microsoft, 2009) – focusing on the stakeholders vendor and customer (in this case operator) of the software product. While STRIDE is utilized here, it is possible to use other threat models. Next, a risk analysis using DREAD is performed – concluding the threat and risk assessment. Again, different risk assessment methods can also be applied. For exampel, regarding the requirement for privacy by design and default, it could be beneficial to consider a privacy threat analysis methodology like LINDDUN (Wuyts et al., 2014). Based on the results from STRIDE and DREAD, a first set of detailed security requirements that mitigate the threats is developed. In order to prioritize the importance of the detailed security requirements, it would make sense to assign a cumulative DREAD risk rating score where the highest risk level of the corresponding STRIDE threat scenario is assigned to the detailed requirement.

In (Ringmann et al., 2018), generic technical requirements are proposed for compliance with the GDPR. This way, the government as a stakeholder is considered with its enforced rules and regulations. From the 74 technical requirements, we select a collection that applies to our application scenario. Based on the selected set of technical requirements, we start a matching process. For each detailed security requirement from the threat and risk assessment, it is checked whether there exists a similar/related technical requirement from the GDPR. This process is done top-down: the GDPR article that first requires something related to a detailed security requirement from the threat and risk assessment is used as a primary source; other articles may have redundant requirements. Matches are entered into an expanded list of detailed requirements. Furthermore, for each technical requirement from the GDPR that has no match from the risk assessment, new, detailed requirements that are needed to fulfill the technical requirement are added to the list. Finally, we further expand the list of detailed requirements by a column for Common Criteria SFRs. Again, for each SFR, it is checked whether there exists a similar/related detailed requirement. Related in this context may also mean that it

Table 1: Stakeholder interests regarding confidentiality (C), integrity (I), availability (A), transparency (T), unlinkability (U), data minimization (M) and intervenability (V).

Stakeholder	Scans of personal data							Data dictionary							Software/Algorithms							Identified personal data						
	C	I	A	T	U	M	V	C	I	A	T	U	M	V	C	I	A	T	U	M	V	C	I	A	T	U	M	V
Vendor	□	■	■	□	□	▨	□	□	■	▨	▨	□	▨	▨	■	■	■	□	□	□	□	□	▨	■	□	▨	▨	□
Customer	■	■	■	■	□	□	□	■	■	▨	■	□	□	□	□	▨	▨	▨	□	□	□	■	■	■	■	□	□	□
Supplier	□	□	■	□	□	□	□	□	□	■	□	□	□	□	□	□	■	□	□	□	□	□	□	■	□	□	□	□
Sender	■	▨	□	■	■	■	■	■	■	□	■	■	■	■	□	□	□	■	■	■	■	■	▨	□	■	■	■	■
Receiver	■	▨	□	■	■	■	■	■	■	□	■	■	■	■	□	□	□	■	■	■	■	■	▨	□	■	■	■	■
Government	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□	□	■	■	■	■	■	■	■	■	■	■	■
L.E.	□	■	▨	■	□	□	□	□	■	■	■	■	■	▨	□	□	□	■	□	□	□	□	■	■	■	□	□	□
Society	■	□	□	■	■	■	■	■	▨	□	■	■	■	■	□	▨	□	■	■	■	■	■	□	□	■	■	■	■

would be beneficial to additionally include the proposals from the SFR into an existing detailed requirement.

5 APPLYING THE METHODOLOGY

Before performing a threat analysis, the interests of the stakeholders must be determined. Based on the work in (Ringmann and Langweg, 2017; Ringmann et al., 2018) we propose to identify stakeholder interests regarding the security principles confidentiality (C), integrity (I) and availability (A) as well as the privacy principles transparency (T), unlinkability (U), data minimization (M) and intervenability by the data subject (V). In context of the application scenario, the following stakeholders must be considered: vendor (data processor), customer/operator (data controller), supplier, sender, receiver (data subject), government, law enforcement (L.E.), society. The resulting matrix of stakeholder interests is displayed in table 1. No interest is represented by white cells, partial interest by grey cells and full interest by black cells. For example, a receiver always has full interest regarding C, T, U, M, and V of all components (except for C of the software). The integrity and availability of the scans and identified personal data are not as important since in case the machine is not working (correctly), manual sorting will still be possible. Regarding the C, I, A of the software/algorithms, the receiver is indifferent.

When having to prioritize which parts of the matrix of interests will be fulfilled by the software, the vendor will implement his own requirements first. Then, the vendor will consider the customer's requirements as these might be essential to be met in order to actually sell the software product. The interests of third parties like sender, receiver, government, and society will be considered to be met for compliance reasons. The GDPR with its possible fines provides a legitimate reason to take a closer look at compliance with relevant rules and regulations enforced by the government.

5.1 STRIDE Threat Analysis

Based on the interests of the stakeholders vendor and cutomer/operator, Microsoft's STRIDE model (Microsoft, 2009) is used for identifying threats to the software. For the application scenario and its components *Scanner*, *Dictionary*,*Software*, and *Identified data* in total 34 threats were identified in (Ringmann and Langweg, 2017). In order to avoid endless tables and briefly provide a demonstrable example of our methodology, in this section and the following, we will only take a closer look at threats in the STRIDE category *Tampering* which are presented in table 2. For the remaining steps of the methodology, we will only consider threat number (TNo.) 13 of the component *Scanner*: "unreadable images of the scanned items through misconfiguration of the scanner's software/hardware".

Table 2: Threats for category *Tampering*.

Component	TNo.	Threat
Scanner	13	Unreadable images of the scanned items through misconfiguration of the scanner's software/hardware
Dictionary	14	Items are sorted incorrectly
Software	15	(incl. underlying components): Software degradation, incorrect sorting, damaged hardware, information disclosure, and unavailability of the system
Identified data	16	Faulty sorting, too many rejects

Table 3: DREAD assessment for category *Tampering*.

Component	TNo.	Threat	Da	R	E	A	Di	Impact (Da+A)/2	Likelihood (R+E+Di)/3	DREAD score	Risk rating
Scanner	13	Unreadable images of the scanned items through misconfiguration of the scanner's software/hardware	1	0	0	1	0	1	0	0.5	Low
Dictionary	14	Items are sorted incorrectly	2	1	2	1	2	1.5	1.67	1.58	Medium
Software	15	Software degradation, incorrect sorting, damaged hardware, information disclosure, and unavailability of the system	2	1	2	1	1	1.5	1.33	1.42	Medium
Identified data	16	Faulty sorting, too many rejects	2	1	1	1	1	1.5	1	1.25	Medium

5.2 DREAD Assessment

Next, the threat scenarios are evaluated according to the associated risks by using the DREAD methodology (Marshall and Hudek, 2018). The DREAD risk score is composed of the mean from impact and likelihood. The impact score builds the average from the DREAD categories *Damage potential* and *Affected users*. The likelihood score is composed of the mean from the categories *Reproducibility*, *Exploitability*, and *Disocverability*. Scores range from 0 to 3. The computations of the risk scores were made utilizing the DREAD score calculator for the Dradis Framework (Martin et al., 2018). Based on the DREAD score, a risk level can be assigned. For the purpose of applying the DREAD methodology to the threat scenarios, the risk rating is assumed as follows:

- **Low**: DREAD score ≤ 1
- **Medium**: $1 <$ DREAD score ≤ 2
- **High**: $2 <$ DREAD score ≤ 3

The scores and risk levels can be assigned in various ways. Since a threat and risk analysis (TRA) is demanded in Article 32 of the GDPR, it makes sense to utilize this initial TRA to document the values and resulting measures, and therefore, already fulfilling a GDPR requirement. An exemplary DREAD assessment for the application scenario and corresponding threats from STRIDE category tampering is presented in table 3. The scores for the application example are estimates and did not involve any real analysis. However, it can be challenging to get all stakeholders involved in the risk assessment process including finding experts who can actually identify threats and evaluate the corresponding risks.

Table 4: Detailed requirements that mitigate TNo. 13.

RNo.	Detailed requirement	TNo.
1	limit physical access to scanner (and other hardware components)	2, 13, 21, 27
13	role-based user management for the software	5, 13, 14, 22, 23
14	definition of an access control policy for the software (role-based)	5, 13, 14, 22, 23
29	software/database(sw): document which roles/users are authorized to read/write/create/modify which resources	13, 16
30	OS: document which users/groups are authorized to read/write/create/modify which resources related to the system	13, 16
31	processes are running only with the allowed privileges (esp. not root)	13, 16, 19
33	limit rights to write/modify files that contain personal data to users/processes that specifically need those rights	13, 14, 15, 16

5.3 Requirements for Threat Mitigation

Based on the threat scenarios, it is necessary to define requirements that mitigate the threats and thus, improve the security of the software product. For the proposed scenario, a complete list of security requirements was developed but cannot be displayed in this paper. Therefore, we will focus on tasks that mitigate threat number (TNo.) 13 of the component *Scanner*: "unreadable images of the scanned items through misconfiguration of the scanner's software/hardware" for the remainder of this paper. Results are displayed in table 4.

These detailed requirements will serve as a first basis for the matching process. While these requirements are based on the interests of the stakeholders vendor and customer/operator, it is necessary to take a look at the requirements from the government imposed through rules and regulations, i.e., the GDPR.

Table 5: Requirements from GDPR for TNo. 13.

GNo	Requirement from GDPR	Article GDPR	Recital GDPR	Further GDPR reference	Matched RNo

1	Secure authentication and authorization mechanisms for all components that allow access to personal data including access to networks, services, and systems	5(1)(f)	39(12)
			49(1-2)
				25(2)
				32(1)(b)
				32(2)
					1

2	Definition of an access control policy on the basis of an identity management where access control is limited to specific roles or attributes (who is allowed to do what with the personal data)	5(1)(f)	39(12)
			49(1-2)
				25(2)	13
					14

8	Limitation of rights for writing or changing files that contain personal data	5(1)(f)		32(1)(b)	31 33
10	Document which roles are authorized to read/write/create/modify which resources	5(1)(f)		32(1)(b)	29 30

5.4 Selection of Applicable Technical Requirements from GDPR

A list of technical requirements from the GDPR was derived in (Ringmann et al., 2018). In the context of this article, it is determined for each technical requirement whether it applies to the planned software project or not. For the utilized exemplary scenario, it was evaluated that only 40 out of 74 requirements have to be fulfilled. The 34 other requirements were either partly not applicable to the software project (e.g., no profiling, data transfer outside of the country), already fulfilled (e.g., threat and risk analysis, auditable documentation of lawfulness), or to be fulfilled by the future operator (e.g., privacy notice, data protection policy, interaction with the data subject). Regarding the minimal application scenario, for threat number (TNo.) 13 the following requirements based on the GDPR are identified in table 5.

5.5 Match Requirements

The matching process is split into two parts. First, for the requirements from GDPR which apply to the software project, it is determined which of the first 50 detailed requirements that resulted from the STRIDE/DREAD analysis match to which applicable requirement from the GDPR. When no match is found, a new entry for a detailed requirement is made. As a result to the existing 50 detailed requirements, 16 more requirements are added. They can also be called technical design measures, as this matching process is the last step from the method KORA that was applied in (Ringmann et al., 2018).

Finally, the matching process is enhanced by yet another dimension. According to Art. 24(3), compliance with a code of conduct or certification may be used to prove lawfulness of certain articles of the GDPR. Therefore, the Common Criteria SFRs that are described in CC Part 2 (Common Criteria, 2017) are evaluated.

The work by (Simić-Draws et al., 2013) applies the KORA method in the context of CC and ISO 27001. It matches the process steps of CC and ISO 27001 to the four process steps in KORA. As a result, the SFRs from CC Part 2 match in the definition part to KORA step 3: definition of technical requirements. The implementation of the SFRs is then considered to be part of KORA step 4: definition of technical design proposals. In the context of this exemplary application scenario, the SFRs are matched to the derived security requirements.

A summary of what is needed for a CC evaluation is also provided by (Simić-Draws et al., 2013). In CC Part 1, the general model is described. As a result, usually a lot more steps need to be taken, e.g., defining the *Target of Evaluation, Evaluation Assurance Level, Security Problem Definition, Security Objectives* before looking at the SFRs. Part of a CC evaluation is to select various SFRs that mitigate threats identified in the *Security Problem Definition* which then need to be proven to be fulfilled by the system to be evaluated. However, for the purpose of matching security requirements in the context of this exemplary application scenario, it suffices to look at the SFRs.

The matching process is then continued by determining for each CC SFR whether there exists a technical design proposal which deals with the kind of requirement. For the reduced application scenario, table 6 presents the detailed requirements for TNo. 13 after the matching process including references to GDPR compliance as well as CC SFRs.

6 CONCLUSION AND DISCUSSION

As a result, we present a list of detailed security requi-

Table 6: Matched detailed requirements for TNo. 13.

RNo.	Detailed requirement	TNo.	GNo.	Article GDPR	Recital GDPR	Further GDPR reference	CC SFRs

1	Limit physical access to scanner (and other hardware components)	2, 13, 21, 27	1	5(1)(f)	39(12), 49(1-2)	25(2)
						32(1)(b)
						32(2)
							FPT_ PHP.1.1

13	Role-based user management for the software	5, 13, 14, 22, 23	2	5(1)(f)	39(12), 49(1-2)	25(2)	FDP_ ACF.1.1 FIA_ USB.1.1 FIA_ ATD.1.1 FMT_ MSA.1.1
14	Definition of an access control policy for the software (role-based)	5, 13, 14, 22, 23	2	5(1)(f)	39(12), 49(1-2)	25(2)	FAU_ SAR.1.1
29	Software/database(sw): document which roles/users are authorized to read/write/create/modify which resources	13, 16	10	5(1)(f)		32(1)(b)	FDP_ ACC.1.1 FMT_ MSA.1.1
30	OS: Document which users/groups are authorized to read/write/create/modify which resources related to the system	13, 16	10	5(1)(f)		32(1)(b)	FDP_ ACC.1.1 FMT_ MSA.1.1
31	Processes are running only with the allowed privileges (esp. not root)	13, 16, 19	8	5(1)(f)		32(1)(b)	
33	Limit rights to write/modify files that contain personal data to users/processes that specifically need those rights	13, 14, 15, 16	8	5(1)(f)		32(1)(b)	

rements that – once implemented – make a software product GDPR-compliant and partially prepared for a CC evaluation. The proposed methodology facilitates the integration of security and privacy by design into the requirements engineering process. Thus, specific, detailed security and privacy requirements are implemented from the very beginning of a software project.

We learned that even for the presented application scenario, the requirements engineering turned out to be quite complex. However, the approach provides a structured way to identify requirements from various sources, match related requirements to avoid duplication and track requirements for compliance assertion. The complexity will be reduced when utilizing requirements engineering tools instead of matrices (e.g., usage of labels, categories, priorities, status of implementation, etc.).

We found that our method uncovered requirements that had previously been unaddressed by the methods in use by the company.

Limitations of this paper refer to the following topics: selection of laws, kind of personal data, kind of certification, redundancy issues, and risk assessment. The GDPR is not the only law that needs to be considered. National data protection laws can be more restrictive or liberating in certain areas, thus, overruling articles stated in the GDPR. Furthermore, other laws might be of importance for a software project, e.g., for the application scenario, postal laws play an important role. Therefore, it may be necessary to apply the KORA method to applying laws in order to identify further requirements. Other projects may need to consider further requirements when processing special categories of personal data or personal data of children. There exist various certification possibilities. While some certifications may be obtained for a product (e.g., Common Criteria), others can only be obtained for the entire organization or its processes (e.g., ISO 27001). Thus, the decision to pursue a certification may not be related to the software project. When certifications are already in place, it must be checked in which ways they already support compliance with laws and regulations. Doing threat assessment requires a certain expertise. The risk rating score is an important property of each requirement. However, it was not possible to disclose further risk values for the application scenario. Regarding requirements for fulfilling privacy by design and by default, further threat modeling should be considered, e.g. in applying LINDDUN (Wuyts et al., 2014). The requirements matching process is vulnerable to redundancy issues which may lead to an increased complexity and a reduced traceablilty to corresponding GDPR articles or requirements from a standard or code of conduct. In conclusion, for each of these limitations further requirements may evolve.

REFERENCES

Amara, N., Huang, Z., and Ali, A. (2019). Modelling security requirements for software development with common criteria. In Wang, G., Feng, J., Bhuiyan, M. Z. A., and Lu, R., editors, *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, pages 78–88, Cham. Springer International Publishing.

Bartolini, C., Lenzini, G., and Santos, C. (2018a). A Legal Validation of a Formal Representation of GDPR Articles. In *Proceedings of the 2nd JURIX Workshop on Technologies for Regulatory Compliance (Terecom)*.

Bartolini, C., Lenzini, G., and Santos, C. (2018b). An interdisciplinary methodology to validate formal representations of legal text applied to the GDPR. In *Proceedings of the Twelfth International Workshop on Jurisinformatics (JURISIN)*.

Basin, D., Debois, S., and Hildebrandt, T. (2018). On Purpose and by Necessity: Compliance Under the GDPR. In Meiklejohn, S. and Sako, K., editors, *Financial Cryptography and Data Security*, pages 20–37, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bräunlich, K., Richter, P., Grimm, R., and Roßnagel, A. (2011). Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA. *Datenschutz und Datensicherheit-DuD*, 35(2):129–135.

Common Criteria (2017). Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components. Version 3.1 Revision 5.

Dewitte, P., Wuyts, K., Sion, L., Van Landuyt, D., Emanuilov, I., Valcke, P., and Joosen, W. (2019). A comparison of system description models for data protection by design. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, SAC '19, pages 1512–1515, New York, NY, USA. ACM.

Hammer, V., Roßnagel, A., and Pordesch, U. (1992). *KORA: Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für IuK-Systeme*. Number 100 in Arbeitspapier. provet.

Jensen, M., Kapila, S., and Gruschka, N. (2019). Towards Aligning GDPR Compliance with Software Development: A Research Agenda. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP,*, pages 389–396. INSTICC, SciTePress.

Kammüller, F. (2018). Formal Modeling and Analysis of Data Protection for GDPR Compliance of IoT Healthcare Systems. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 3319–3324.

Kammüller, F., Ogunyanwo, O. O., and Probst, C. W. (2019). Designing Data Protection for GDPR Compliance into IoT Healthcare Systems. *arXiv e-prints*. arXiv:1901.02426v1.

Lopes, I. M., Guarda, T., and Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6.

Marshall, D. and Hudek, T. (2018). Threat modeling for drivers. last accessed on 2019-07-19.

Martin, D., Villa, X., Bogner, T., and Manaloto, A. (2018). DREAD score calculator for Dradis. Version 3.11.0.

Microsoft (2009). The STRIDE Threat Model. https://msdn.microsoft.com/en-us/library/ee823878 (v=cs.20).aspx. Last accessed on 2019-08-21.

Nissim, K., Bembenek, A., Wood, A., Bun, M., Gaboardi, M., Gasser, U., O'Brien, D., Steinke, T., and Vadhan, S. (2018). Bridging the gap between computer science and legal approaches to privacy. In *Harvard Journal of Law & Technology*, volume 31, pages 687–780. Harvard Journal of Law & Technology, Harvard Journal of Law & Technology.

Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., and Robaldo, L. (2018). PrOnto: Privacy ontology for legal reasoning. In Kő, A. and Francesconi, E., editors, *Electronic Government and the Information Systems Perspective*, pages 139–152, Cham. Springer International Publishing.

Pandit, H. J., Fatema, K., O'Sullivan, D., and Lewis, D. (2018a). GDPRtEXT - GDPR as a Linked Data Resource.

Pandit, H. J. and Lewis, D. (2017). Modelling Provenance for GDPR Compliance using Linked Open Data Vocabularies. In *Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn)*.

Pandit, H. J., OSullivan, D., and Lewis, D. (2018b). Queryable provenance metadata for GDPR compliance. *Procedia Computer Science*, 137:262–268.

Ringmann, S. D. and Langweg, H. (2017). Determining security requirements for cloud-supported routing of physical goods. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 514–521. IEEE.

Ringmann, S. D., Langweg, H., and Waldvogel, M. (2018). Requirements for Legally Compliant Software Based on the GDPR. In Panetto, H., Debruyne, C., Proper, H. A., Ardagna, C. A., Roman, D., and Meersman, R., editors, *On the Move to Meaningful Internet Systems. OTM 2018 Conferences*, pages 258–276. Springer International Publishing.

Simić-Draws, D., Neumann, S., Kahlert, A., Richter, P., Grimm, R., Volkamer, M., and Roßnagel, A. (2013). Holistic and law compatible IT security evaluation: Integration of common criteria, ISO 27001/IT-Grundschutz and KORA. *International Journal of Information Security and Privacy*, 7(3):16–35.

Sion, L., Dewitte, P., Van Landuyt, D., Wuyts, K., Emanuilov, I., Valcke, P., and Joosen, W. (2019). An architectural view for data protection by design. In *2019 IEEE International Conference on Software Architecture (ICSA)*, pages 11–20.

Wuyts, K., Scandariato, R., Joosen, W., Deng, M., and Preneel, B. (2014). LINDDUN privacy threat modeling. https://linddun.org/index.php. Last accessed 2019-10-22.

Yin, L. and Qiu, F. (2010). A novel method of security requirements development integrated common criteria. In *2010 International Conference On Computer Design and Applications*, volume 5, pages V5–531–V5–535.