Requirements for legally compliant software based on the GDPR

(⌧) Sandra Domenique Ringmann[1,2,3], Hanno Langweg[2,4], and Marcel Waldvogel[3]

[1] Siemens Postal, Parcel & Airport Logistics GmbH, Konstanz, Germany
[2] HTWG Konstanz University of Applied Sciences, Konstanz, Germany
sandra.ringmann(at)htwg-konstanz.de, hanno.langweg(at)htwg-konstanz.de
[3] University of Konstanz, Konstanz, Germany
[4] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU, Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. We identify 74 generic, reusable technical requirements based on the GDPR that can be applied to software products which process personal data. The requirements can be traced to corresponding articles and recitals of the GDPR and fulfill the key principles of lawfulness and transparency. Therefore, we present an approach to requirements engineering with regard to developing legally compliant software that satisfies the principles of privacy by design, privacy by default as well as security by design.

Keywords: requirements engineering · GDPR · compliant software · security by design · privacy by design and by default.

1 Introduction

The General Data Protection Regulation (GDPR) entered into force on 24th of May 2016 and the transition period ended on 25th of May 2018, making the rules applicable in all member states of the European Union. It has attracted attention world-wide, across all industries. As a result of the territorial scope defined in Article 3 of the GDPR, more companies must be compliant with the GDPR, e.g., especially referring to companies that process personal data which was acquired over the internet. Furthermore, the GDPR specifically requires that processing of personal data must comply with the GDPR and this compliance must be verifiable. This is postulated through the principles of lawfulness and transparency, for example, in Art. 5(1)(a).

Most data processing is done with the help of software – either with human interaction or fully automated. Therefore, it makes sense to have a look at the software development process in the context of the GDPR. At the beginning of each software development life cycle, requirements are gathered and defined by taking into account various stakeholders. According to [23], the government, i.e., by enforcing laws and regulations is one of the stakeholders to be considered.

Applying the principles of lawfulness and transparency of the GDPR, it must be provable that the software which processes personal data is compliant with the rules laid down in the GDPR. However, the requirements defined in the articles and paragraphs of legislative texts are usually not serviceable for requirements engineering in software development.

In contemplation of being able to define reusable requirements for software development, we define the scope for which this research applies. The first limitation is that we keep the definition of technical requirements generic in order to be able to have reusable software requirements which can be applied to all kinds of software. Second, we do not specify any purpose for which software is developed, whether the software is developed by a potential data processor or controller, whether the personal data processed is that of an end-user of the software, or whether personal data is to be transferred to third countries or international organizations. Third, we do not consider special categories of personal data nor processing of personal data of children. Fourth, we leave out any additional or altered requirements that could result from taking into account national laws for data protection or any other laws that might need to be considered for the software. The main goal of this research is to define technical requirements that need to be implemented to make software compliant with the GDPR and being able to trace which legal requirements from the GDPR are fulfilled with these technical requirements. A detailed application example that illustrates the various requirements is not in scope of this paper and will be part of future research.

The remainder of this paper is structured as follows. Section 2 provides an overview of the related work. Then, the methodology is described. Section 4 contains the technical requirements that were derived from the GDPR. In section 5 we look at the impact of the identified requirements on stakeholder interests. Then, we discuss the findings in section 6 and conclude with an outlook on future work in section 7.

2 Related Work

Our work relates to the research areas requirements reuse and regulatory compliance in software systems. Furthermore, previous work on the methodology and with regard to the GDPR is considered.

2.1 Reusable Requirements

Reusing requirements for a software product is a beneficial strategy that leads to improved productivity and quality in the software development process and the product obtained [27]. The definition of security requirements is suited well for reusability because software often faces similar threats and mitigation techniques are quite standardized [7].

In [26, 25], Toval et al. develop the requirements engineering method SIREN (SImple REuse of software requiremeNts) and specify templates for reusable requirements regarding security as well as data protection based on the Spanish implementation of the European Data Protection Directive 95/46/EC. Correspondingly, the work by [20] applies the Norwegian implementation of the EU Directive 95/46/EC to identify reusable security requirements for health-care applications. The work by [7] presents the methodology SQUARE (Security Quality Requirements Engineering) that contains a nine-step process for identifying, classifying, and prioritizing reusable security requirements. Our work proposes a different methodology for identifying reusable security and personal data protection requirements with regard to the GDPR which replaces the national implementations of the EU Directive 95/46/EC.

2.2 Regulatory Compliance

Continuing with the topic of requirements engineering, it is essential to verify that specified requirements are compliant with applicable laws and regulations. A research overview on how laws and regulations have been handled in the context of software development is given by [22]. Methodologies that deal with requirements engineering and regulatory compliance are proposed in [2, 5, 9]. In this paper, we identify technical requirements that can be traced back to the legal requirements from which the technical requirements were derived using the method KORA. Thus, verification of compliance is given if it can be demonstrated that an information system satisfies the technical requirements.

2.3 KORA

KORA is a method that was introduced by [14] and has been used in German legal research. KORA is the abbreviation for "Konkretisierung rechtlicher Anforderungen" (concretization of legal requirements). In [16, 17], a short description and exemplary applications are provided. KORA is used to derive requirements for information systems. [4, 24] are further works where KORA is applied in the context of the *Common Criteria*. KORA is the method that is used in this research to derive technical requirements from legal requirements.

2.4 GDPR-specific Research

The report by the European Union Agency for Network and Information Security (ENISA) [10] on privacy and data protection by design focuses on the implementation of the privacy properties transparency, unlinkability, data minimization and intervenability. It provides an overview of existing approaches regarding privacy design strategies and the utilization of privacy-enhancing techniques. Security and privacy properties have been investigated by [21] in the cloud context, not yet referring to the GDPR. The Standard Data Protection Model (SDM) [1] takes into account all data protection goals defined in the GDPR and can be applied as a tool for identifying and assessing technical and organizational measures (TOMs) as well as performing a risk analysis.

The process of when which articles from the GDPR apply, can be mapped by petri nets (visualization technique). This is suggested by [11] where petri nets are utilized to model the legal process and the software process in order to achieve privacy by design and compliance with the GDPR. Legal requirements that result from the GDPR are investigated by [6]. The work is similar to our proposal. However, the research by [6] is limited to listing legal requirements in the security context related to big data. Furthermore, we identify generic legal requirements and technical requirements with regard to developing a software product.

3 Methodology

KORA is a method that bridges the gap between abstract legal requirements and concrete technical requirements. We use KORA to identify software requirements from the GDPR. We decided to use this method because it fits the purpose best: it is well established, it can be used with little knowledge in the legal area, it is straightforward to use and it matches the abstraction level of requirements engineering. The method consists of four steps:

1. definition of legal requirements through selection of relevant articles from applicable laws
2. determination of legal criteria for IT systems based on identified legal requirements
3. derivation of technical requirements from legal criteria, yielding functional and non-functional characteristics of an IT system
4. creation of technical design proposals based on the technical requirements

First, from applicable laws the relevant articles and paragraphs are selected as legal requirements. In the context of this research, we only examine the 99 articles of GDPR [12]. Based on the legal requirements, we determine legal criteria by describing implications of the legal requirements with regard to an information system. The 173 recitals of the GDPR [13] guide the articles and can serve as a first basis to derive legal criteria. In the future, it could also be that court decisions will contribute further and more detailed legal criteria. From the legal criteria, we can identify technical requirements that will specify functional or non-functional characteristics of an information system. Some sentences of the articles in the GDPR are very specific and can directly serve as technical requirements. In other cases, the help of recitals and interpretations is necessary to identify technical requirements. We used the interpretations in [1], [3] and [19] as well as our own expertise to define the technical requirements and also identify which parts of which articles and recitals were relevant for which categories of requirements. As a last step, technical design proposals would be made that fulfill the technical requirements and serve as a guideline to implement the technical requirements. We find that this last step is hard to generalize as it is depending on the utilized programming languages, frameworks and libraries. Therefore, we limit our goal to deriving reusable technical requirements from the GDPR.

The key principles relating to processing of personal data within the GDPR are: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability (Art. 5). To have a better overview of the kinds of requirements that can be derived from the GDPR, we classified the requirements into categories. The categories we defined are similar to the key principles but summarize some of the principles and add the categories availability and data transfer. As an orientation served [1] and [10]. Many paragraphs of articles refer to multiple categories, thus, creating redundancy issues. When requirements are present in other categories, references are made accordingly. All references to articles and recitals are from the GDPR.

4 Technical Requirements Based on Legal Requirements

4.1 Confidentiality

The data protection goal confidentiality arises particularly from Art. 5(1)(f), Art. 28(3)(b) and Art. 32(1)(b). Furthermore, Articles 25(2), 29 and 32(2) play a role in this context. Confidentiality is supposed to ensure that no unauthorized or unlawful processing of data takes place. A violation of confidentiality usually also violates the principle of lawfulness that is discussed in section 4.9. [1, 18]

The content of Art. 5(1)(f) is enhanced by Recitals 39(12) and 49(1-2). We identify the following legal criteria:

- protection against unauthorized and unlawful processing (Art. 5(1)(f))
- protection against unauthorized access to or use of personal data in storage or transition as well as access to networks and services that process this data (Recital 39(12) and 49(1-2))
- protection against accidental loss (data disclosure) (Art. 5(1)(f))
- ensure network and information security (Recital 49(1))
- identify TOMs for ensuring confidentiality, thus, implementing an appropriate security of personal data (Art. 5(1)(f) and Recital 39(12))

From the legal criteria, we deduce technical requirements as follows [1, 21]:

- secure authentication and authorization mechanisms for all components that allow access to personal data including access to networks, services, and systems
- definition of an access control policy on the basis of an identity management where access is limited to specific roles or attributes (who is allowed to do what with the personal data)
- depending on the location and accessibility of the data, it should be considered to encrypt all data at rest and/or in motion

Art. 28(3)(b) refers to the processor's responsibility to ensure confidentiality of personal data. Along with Art. 29, requirements are of a contractual nature between controller and processor and should not be interpreted into technical requirements for a software product.

Art. 32(1)(b) along with Recital 83(2-3) require TOMs for state-of-the-art, ongoing confidentiality of processing systems and services. Moreover, a risk analysis is expected and in case the risk is found to be "high", a data protection impact assessment according to Art. 35 must be carried out. Risk in combination with confidentiality is also treated by Art. 32(2) in conjunction with Recital 75. Therefore, we can conclude that a threat and risk analysis must be conducted. In general, Recitals 84, 89, 90, 91 and 95 contain more information on the data protection impact assessment. In the context of confidentiality, risk assessment for unauthorized disclosure or access to personal data transmitted, stored or otherwise processed is of importance. Based on the results of the threat and risk analysis, further technical requirements will have to be defined.

From Art. 25(2) and the corresponding Recital 78, the necessity for authentication and access control can be deduced which is covered by Art. 5(1)(f). Furthermore, the article refers to the implementation of TOMs to ensure data protection by design and default.

It can be summarized that the following mechanisms are necessary for the fulfillment of the confidentiality data protection goal: authentication, authorization, access control and encryption of personal data. Further measures may result from risk analysis including the identification of TOMs.

4.2 Integrity

The goal to guarantee integrity of data is regulated primarily by Art. 5(1)(f) and 32. For Art. 5(1)(f), we identify some further legal criteria and technical requirements regarding the integrity of data. As already mapped out in the previous section, authorization and access control are essential. In the context of integrity, Art. 5(1)(f) along with Recital 49(1-2) expects protection against damage and unauthorized erasure or modification of data. Again, TOMs for ensuring integrity need to be defined. TOMs are always underpinned by Art. 25(1) in general and by Art. 32(1) regarding security and risk assessment. Therefore, Art. 32(1)(b) in combination with Recital 83(2) require TOMs for state-of-the-art, ongoing integrity. From Art. 32(2), an obligation for a risk assessment regarding accidental or unlawful destruction, alteration or loss is derived as a legal criterion. Results from the risk analysis will serve as additional technical requirements. From Art. 5(1)(f) we deduce further technical requirements [1, 21]:

- limitation of rights for writing or changing files that contain personal data
- check the integrity of data before, during and/or after processing the data, utilizing signatures, check-sums or electronic identifiers
- document which roles are authorized to read/write/create/modify which resources
- define and implement processes for maintenance and timeliness/up-to-dateness of data
- define the expected behavior of processes, make regular tests and document whether the full functionality is still available

In summary, mechanisms for limiting access to data as well as ensuring the integrity of data and processes must be implemented. Further measures may result from risk analysis including the identification of TOMs.

4.3 Availability

The availability of a system and data within that system is postulated in Art. 32(1)(b,c,d) in the context of secure processing. In Art. 5(1)(e), the availability of data is a requirement for the identification of the data subject. However, availability of data is limited to the necessity/purpose of processing. Art. 13(2)(a), 15(1) and 20(1,2) deal with the controller's duty to inform about and provide access to a user's personal data. [1, 18]

From Art. 32(1)(b) in combination with Recital 49, we can identify the legal criterion to apply TOMs for state-of-the-art, ongoing availability and resilience of processing systems. This includes "...ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions..." (Recital 49(1)). Technical requirements then include DoS protection, intrusion prevention, as well as input validation (prevent malfunctioning of the system). Prior to determining the technical requirements, a risk assessment regarding availability is necessary. The results of the risk assessment can alter or demand additional technical requirements. This is also the case for the following legal requirement.

Art. 32(1)(c) refers to incident handling. It requires "...the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;". Along with Recital 83(3), it can be concluded that there is need for incident detection, a process for incident handling (to restore availability), backup & restore as well as disaster recovery.

Art. 32(1)(d) requires that security of processing is always assured. Thus, the TOMs implemented for system security must be regularly reviewed. Technical requirements in this context must be defined depending on the TOMs implemented for assuring security of processing. For example, a process that takes into account vulnerability and patch management as well as progress of the state-of-the-art could make this requirement compliant. Art. 32(1)(d) is also referenced in sections 4.6 and 4.9.

Art. 5(1)(e) calls for limited storage duration of personal data, see also sections 4.4 and 4.5. In the context of availability, this means that personal data must only be available for the time that it is needed for processing. Art. 5(1)(e) in accordance with Recital 39(10) demands that a time limit is defined after which data is either erased because it is no longer needed for processing or a review is made that assesses whether data is still needed for processing. A review would need to be repeated periodically after the defined time limit. If personal data is to be kept longer than needed for processing purposes as allowed in Art. 5(1)(e), e.g., for statistical, archiving, scientific, or historical purposes, it must be altered using, i.e., pseudonymization (see Art. 89(1), 25(1), 32(1)(a), 40(2)(d), 6(4)(f) as well as Recitals 28 and 78).

Art. 13(2)(a) builds upon Art. 5(1)(e) and further requires the controller to tell the data subject for how long the personal data will be stored (or be available) "... or if that is not possible, the criteria used to determine that period;". This last part of the sentence may alleviate the first part when companies would then just inform the data subject that storage of the personal data will be as long as some sort of processing for some sort of purpose is necessary. Thus, there is an "either-or" technical requirement to comply with this part of Art. 13. Either, there is a defined period after which data is deleted. Or, there are defined criteria that would determine when data must be deleted when no fix period can be determined.

Art. 15(1) and Art. 20(1,2) deal with providing access to a data subject's personal data. Art. 15(1) along with Recital 63 give the data subject the right to find out whether a controller is processing personal data concerning the data subject. Therefore, the technical requirement to be able to search for a potential data subject's identity can be deduced. Furthermore, if the inquiry of the data subject is positive, the controller would need to give the data subject access to its data. This can be accomplished as described in Art. 20. In case of a large amount of data, the software would also need to be able to filter for data categories (see Recital 63(7)). Art. 15(1)(a-h) moreover requires the controller to inform the data subject, e.g., for which purposes processing takes places, which categories of personal data are involved in the processing, for how long personal data is stored, whether processing includes automated decision making as well as how rectification or erasure of data or a complaint about the controller can be made.

Art. 20(1)(a,b) as well as Recital 68(3-6) specify under which processing conditions Article 20(1) applies. In case it applies to the way data is processed in the software, Recital 68 and, in addition, Art. 20(2) further describe the controller's responsibility to send a collection of the processed personal data to the data subject. Therefore, there exist the following technical requirements:

- export function for sending collection of personal data to a data subject (Art. 20(1), Recital 68(1))
- the format of the exported data must be commonly used, machine-readable and inter-operable (in order to move data to another controller) (Art. 20(1), Recital 68(1-2))
- if technically feasible: export function that sends collection of personal data to another controller (Art. 20(2), Recital 68(10))

Measures for assuring availability are split into two categories. On the one hand, availability refers to the system and its corresponding components. On the other hand, the personal data of the data subject must be made available to him or her. Further measures may result from risk analysis including the identification of TOMs.

4.4 Unlinkability

The data protection goal unlinkability is requested particularly through Art. 5(1)(b) "purpose limitation". Unlinkability in this context refers to the obligation to process data only for the purposes that the data was collected for. This is also dealt with in points (c) and (e) of Art. 5(1). If further processing is wanted that goes beyond the initial purposes, Art. 6(4) must be applied. Any kind of automated individual decision-making (including profiling) that is used during processing of personal data is regulated by Art. 22. Pseudonymization is acknowledged as a suited method for assuring unlinkability (see previous section for article references). [1, 18]

Art. 5(1)(b) in accordance with Recital 39(6) and Art. 5(1)(e) demand an extended definition of the data life cycle (see section 4.6) where it should be documented during each stage of the data life cycle that the purpose for which the data is processed, is specific, explicit and legitimate. Art. 5(1)(c) along with Recital 39(9) further require documentation that the "purpose of the processing could not reasonably be fulfilled by other means". Art. 5(1)(c,e) also refer to data minimization and are further covered in section 4.5.

Art. 6(4) must only be considered if processing beyond the initially agreed-upon purposes that the data subject consented to (or any of the other grounds defined in Art. 6(1)(a-f) – see section 4.9). Therefore, in addition to having defined the data life cycle, it would also be necessary to prove that data is following the defined life cycle and document that this life cycle is in accordance to the lawfulness of processing as defined in Art. 6(1)(a-f). If Art. 6(4) has to be applied, it would be required to document and assess that "processing is compatible with the purposes for which the personal data were initially collected" (Recital 50(1)). Points (a-e) of Art. 6(4) and Recital 50(6) define the scope of the assessment.

Art. 22 must be applied if data processing includes automated individual decision-making, including profiling. Paragraph 1 actually gives the data subject "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". This is further interpreted in Recital 71(1-2). Exceptions to paragraph 1 of Art. 22 are defined in paragraph 2. In case points (a) or (c) from paragraph 2 apply, we can then derive the technical requirement from paragraph 3 along with Recital 71(4) to implement safeguards regarding automated processing by at least being able to intervene manually in the processing activities.

Art. 25(2) in accordance with Recital 71(6) and 60(3) in the context of possible profiling activities requests to use appropriate mathematical or statistical procedures for the profiling, use TOMs to prevent data inaccuracies, secure personal data, prevent that profiling activities have discriminatory effects and inform the data subject that profiling activities take place and which consequences they have.

It can be summarized that besides documentational requirements, further measures to satisfy the unlinkability data protection goal must only be taken if automated individual decision-making or profiling is involved.

4.5 Data Minimization

The goal of data minimization is closely linked to unlinkability. Similar articles apply. Art. 5(1)(c) in accordance with Recital 39(7-8) are the main contributors to data minimization. It is demanded, that "the period for which the personal data are stored is limited to a strict minimum"(Recital 39(8)). Therefore, it can be deduced that personal data must be deleted – or, as postulated in Recital 39(10), periodically reviewed – after a defined amount of time. This should be provided as a function within a software product. Furthermore, as few data as needed should be collected and processed. Therefore, the documentation of the data life cycle should also include an assessment regarding data minimization. The requirement for Art. 5(1)(e) was already covered in the context of availability, see section 4.3. Art. 25(2) along with Recital 78(2-3) refers to data minimization as a measure to show compliance to data protection by design and data protection by default.

4.6 Transparency

The principle of transparency is one of the main goals of the GDPR. Important Articles include Art. 5(1)(a) as well as the obligation to provide information stipulated in Articles 12 through 14. [1, 19] There is even a separate Recital for transparency (Recital 58). Transparency will mostly involve either documentation to prove lawfulness or providing information to the data subject or supervisory authority. This information is to be "concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used."(Recital 58(1)) Therefore, requirements will be of a non-functional nature regarding documentation unless information is to be displayed through the software.

Art. 5(1)(a) deals with transparency regarding the processing of personal data. Recital 39(2-4) further describes how this can be done and which information must be provided. Two requirements can be deduced: transparent processing of personal data is to be documented in the data life cycle and a privacy notice must be defined. The second requirement is a document of a contractual nature and should only be included in the technical requirements if displaying the privacy notice and having the user consent to it before transferring any personal data is to be part of the software. Working out this document will be done by legal experts. Regarding the presentation, Recital 60(5-6) states: "That information may be provided in combination with standardized icons in order to give an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable." The requirement for a privacy notice and its content is clarified further in Art. 12, 13, 14 as well as Recitals 60, 61, 62.

Art. 15(1) was already covered in section 4.3 and will be dealt with again in section 4.7. Art. 19 requires the controller to notify the data subject about rectification, erasure or restriction of processing regarding his/her personal data. This will also be covered by section 4.7.

Art. 25(1) and 25(2) refer to privacy by design and privacy by default. In the context of the transparency principle, it must be specified which requirements are defined to fulfill the demand for privacy by default and which requirements are defined to fulfill the demand for privacy by design. Furthermore, it should be checked whether the specified requirements are sufficient or whether more measures (e.g. TOMs) are necessary to reach compliance (Recital 78(2)).

Art. 30 in accordance with Recital 82 requires that processing activities are to be recorded by the controller and, where applicable, by the processor. Art. 30(3) states that the documentation must be in writing, including in electronic form. Paragraph 5 outlines exceptions for having to document all processing activities. The documentation stays internal unless, as stated in paragraph 4, the supervisory authority requests those records. Paragraphs 1 and 2 define the content of the records for the controller (paragraph 1) and the processor (paragraph 2). The information is similar to the one provided in the privacy notice and data life cycle. The records contain information from different stakeholders. Thus, the non-functional technical requirement would be to create those records. If records are to be created automatically by the software, a functional technical requirement would need to be defined further. According to Art. 30(1)(g) and 30(2)(d), one rather interesting part of the record is to document the implemented TOMs as referred to in Art. 32(1).

Art. 32(1)(d) along with Recital 74(1-3) require transparency and documentation regarding the assurance of the security of processing. Art. 32(1)(d) also relates to section 4.9 and 4.3. Here, the GDPR basically states the technical requirement within the legal requirement. There must be "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing". The definition leaves quite some room for interpretation. Taking the perspective of a security professional, the requirement could include the following measures:

- continuous testing for software vulnerabilities
- regular installation of patches (software product as well as operating system)
- vulnerability management (which vulnerabilities exist, which new vulnerabilities are found, when are patches available, when are patches installed/implemented in which versions)
- re-testing all security requirements for new releases as well as re-evaluating whether new security requirements may have evolved through progress in, e.g., state-of-the-art

Art. 33(5) and Recital 87 refer to data breaches. In case of a personal data breach, documentation must include: facts relating to the breach, its effects and the remedial action taken. Furthermore, the documentation serves as proof of compliance for the supervisory authority. This requirement is related to incident handling which was covered in section 4.3. Therefore, the technical requirement would be to have the incident handling process as such that in case of a personal data breach, documentation of the incident is compliant with Art. 33.

In summary, satisfying the principle of transparency requires mostly appropriate documentation as well as providing information to the data subject or supervisory authority.

4.7 Intervenability

The data subject's right to intervene in the processing activities of the data controller/processor emerges mainly from the right to rectification (Art. 16), erasure

(Art. 17), restriction of processing (Art. 18), object (Art. 21) as well as the right to data portability (Art. 20, has already been covered in section 4.3). In this context, Art. 5(1)(d) requires the data processor/controller to create the necessary conditions for granting these rights to the data subject.[1, 19] According to Art. 5(1)(d), the data processor/controller must ensure that personal data is accurate. If personal data is found to be inaccurate, it must either be erased or rectified. This is also stipulated in Recital 39(11). Therefore, there are multiple requirements that can be deduced: data is to be kept up to date when necessary (thus, optional requirement); there ought to be some kind of process that checks regularly for erroneous data (without exceeding the purpose for which they are processed); if faulty data are found, there should be a way to either rectify or delete the data manually or automatically as soon as possible.

Art. 13(2)(c) and Art. 14(2)(d) require the controller to inform the data subject about the possibility to withdraw consent (only if processing is based on Art. 6(1)(a) or Art. 9(2)(a), see section 4.9). This is usually part of the privacy notice (see section 4.6). The difference between Art. 13 and 14 is that Art. 13 refers to data that has been directly obtained from the data subject while Art. 14 refers to data that has not been directly provided by the data subject.

Art. 15(1) was already covered in section 4.6 and deals with the data subject's right to information on and access to personal data concerning him or her. In the context of intervenability, Art. 15(1)(e) gives the data subject the right to rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), as well as objection to processing (Art. 21) and access to the data (Art. 15(1)). The requirements resulting from the afore-mentioned articles all have the precondition that the data subject contacts the data controller with a certain request regarding his or her personal data. Therefore, the software product must be able to provide certain functionality upon request.

For Art. 15 through 21 (except Art. 20) and the corresponding Recitals, we can identify the following technical requirements:

- provide direct access to the data subject's personal access through a remote access to a secure system, if feasible (Art. 15(1), Recital 63(4))
- provide a copy of the personal data that is processed upon request by the data subject (Art. 15(3))
- correct faulty data and complete incomplete data upon request by the data subject (Art. 16, Recital 65(1))
- erase personal data upon request by the data subject (Art. 17(1), Recital 65(2))
- erase also any links to, copy or replication of personal data that was requested to be erased, including informing other controllers that are processing this data (Art. 17(2), Recital 66)
- have a process for erasing data as soon as one of the following occasions in Art. 17(1)(a-f) occur (also in Recital 65(2-4)); exceptions to those occasions are pointed out in Art. 17(3)
- restrict the processing of a data subject's personal data if requested or otherwise mandatory through application of Art. 18(1); Recital 67(1-3) provides

proposals how to achieve the restriction of data processing – how this restriction is implemented is dependent on the software product and cannot be generalized

- inform the data subject about any activities regarding rectification, erasure or restriction of processing (Art. 18(3), 19)
- stop processing of a subject's personal data if the data subject objects to it (Art. 21(1) sentence 1) or prove and document that, as described in Art. 21(1) sentence 2 and Recital 69(1-2), there exist "compelling legitimate grounds for the [continuing] processing"

In summary, intervenability of the data subject requires that the controller or processor is able to erase, rectify or restrict the processing of personal data upon request by the data subject. Moreover, this category includes requirements regarding the handling of faulty data.

4.8 Data Transfer by the Controller

In contrast to the data subject moving his/her data, the controller may also have an interest in transferring data across territorial boundaries. This is, for example, an important topic for cloud deployments. Therefore, requirements in this section are to be seen as optional, applicable only if data is transferred to third countries or international organizations. Chapter 5 of the GDPR covers this topic mostly.

Art. 45(1) in accordance with Recital 103 allow data to be transferred without any specific authorization to third countries or international organizations if they have been approved of by the European Commission (i.e., such that an adequate level of protection of the data is ensured). Therefore, the (technical) requirement can be determined to check and document whether the country/organization is part of the approved ones by the European Commission.

If the country/organization has not been approved, Art. 46 must be applied and appropriate safeguards as described in Art. 46(2,3) as well as Recital 108 must be undertaken. Art. 15(2) gives the data subject the right to be informed about the safeguards that have been implemented in case of a data transfer across territorial boundaries. The technical requirement then to be fulfilled is to document, determine and implement safeguards necessary to assure compliance with data protection requirements (i.e. key principles regarding data processing and data protection by design and by default) as well as assuring that data subjects have appropriate rights with regard to processing in that third country or international organization.

Art. 30(1)(d,e) and 30(2)(c) demand documentation of any processing activities where data has been disclosed to recipients in third countries or international organizations. This relates to the recording of any processing activities covered in section 4.6 and should be included in that requirement in case of data transfers to third countries or international organizations.

4.9 Lawfulness/Accountability/Fairness

Lawfulness is one of the basic principles for processing data. It is the main reason why we have started this research. Lawfulness referring to data processing is demanded throughout the entire GDPR, starting with Art. 5(1)(a). As soon as personal data is processed, the GDPR applies (Art. 1,2). Failure to comply with the basic principles for processing as demanded in Art. 5 may lead to substantial fines as defined in Art. 83(5)(a).

In Art. 6(1), the GDPR differentiates between the following lawful bases that can be selected for data processing: consent, contractual necessity, legal obligation, vital interests, public interest and legitimate interests [18] . Depending on the ground for processing personal data, various constellations of requirements resulting from the application of differing articles and recitals occur. We do not explore this topic further at this moment because it is very individual depending on the software product and type of personal data to be processed. In addition, more legal expertise in that specific domain is necessary. However, we can conclude one technical requirement from Art. 6(1): select and document the reasons for choosing a legal ground for processing personal data.

Art. 5(1)(a) in accordance with Recital 39(1) require processing to be lawful and fair. Fairness in this context means that data processing must not be done "in a way that is unduly detrimental, unexpected or misleading to the individuals concerned" [19, 18]. Further, taking into account Art. 5(2), which demands to be responsible and to be able to demonstrate compliance with the key principles for data processing, we can deduce the technical requirement to have auditable documentation of lawfulness for every legal requirement which applies. This is what we try to achieve in this research by selecting general legal requirements that would apply to most software products that process personal data and mapping these legal requirements to technical requirements.

Continuing with the principle of lawfulness, Art. 24(1) along with Recital 78 demand that TOMs are implemented in order to ensure compliant processing. Again, the demonstrability of these measures is required including further the review and update of TOMs. Therefore, a possible technical requirement that satisfies the legal requirement/criterion would be to demonstrate for each software version that compliance to current legislation is guaranteed.

Art. 24(2) requires the controller to have a data protection policy. The definition of a data protection policy is found in Art. 4(20) 'binding corporate rules'. However, this requirement is not a strict one as it applies only "where proportionate in relation to processing activities". Therefore, a non-functional technical requirement would include either the documentation of the data protection policy or the documentation of why it is not "proportionate" to have a data protection policy. Both requirements are of a contractual/legal nature. The requirement for the data protection policy can be of a functional nature if displaying it and having the user consent to it before transferring any personal data is to be part of the software.

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, some of the previously identified requirements may be obsolete as they will be fulfilled through adherence to the code of conduct or certification. Art. 33(5) deals with lawfulness in case of a data breach. It has already been covered in section 4.6 where the requirement already includes that compliance to the article must be verifiable. Art. 35(11) requires to review the data protection impact assessment which has been part of a requirement in sections 4.1, 4.2 and 4.3. Art. 37(7) which demands to publish contact details of data protection officer has also been covered in section 4.6.

It can be summarized that the key principle of lawfulness requires documentation of regulatory compliance.

5 Stakeholder Requirements

For requirements engineering, it must be clear who the stakeholders are. The requirements identified in the preceding section can serve as a first basis for defining requirements with regard to the government as a stakeholder, taking the government as a representative for applicable laws and regulations. Software usually consists of multiple components that communicate over interfaces. Hence, in our previous work [23], we proposed a method to identify the stakeholders' interests for each software component/interface regarding the security properties confidentiality (C), integrity (I) and availability (A). While the matrix was generated with a specific software product and stakeholders in mind, the method can be applied to any requirements engineering process where stakeholders and their interests should be included. Having now a broader view on the legal requirements, we found it necessary to expand the matrix with the privacy properties transparency (T), unlinkability (U), data minimization (M) and intervenability by the data subject (V) with respect to personal data. An exemplary matrix is displayed in table 1 where stakeholder interests of the vendor and the government (through laws) regarding the security and privacy properties are matched to processing of personal data in interfaces of a software product, for example, source code (as part of intellectual property) and identified personal data. No interest is represented by white cells, partial interest by grey cells and full interest by black cells.

The technical requirements that were identified in section 4 must be broken down according to their applicability to system components and data that is to be processed. Based on this matrix, it should be determined which requirements must be fulfilled in the context of which component/interface. Hence, we need to sort out and match those technical requirements regarding the security and privacy properties for each system component. This is out of scope in the context of this paper and will be part of our future work.

6 Discussion

The scope of this paper is limited since we wanted to keep the requirements as universally applicable as possible. Neither data of children nor special categories

	Source Code							**Identified personal data**						
Stakeholder	C	I	A	T	U	M	V	C	I	A	T	U	M	V
Vendor	■	■	■						▨	■		▨	▨	
Government				■	■	■	■	■	■	■	■	■	■	■

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

of personal data were taken into account. Furthermore, the national laws were not considered. National laws will be important when it comes to data transfers, for example, when software processes personal data in the cloud in a different country than the data was collected in. The GDPR leaves room for national laws to be more restrictive or liberating in certain areas, thus, overruling articles stated in the GDPR.

Specific requirements resulting from a threat and risk analysis as well as identified technical and organizational measures (TOMs) in the context of privacy by design, privacy by default as well as security by design remain unclear. In Germany, as a result of and in addition to the application of the Standard Data Protection Model [1], there should have been a publication of measures and modules since the end of May 2018. These measures and modules could be an initial set of TOMs. However, no publication was made so far [15]. In the context of privacy by design and privacy by default, the works by [8, 10, 11] serve as a good starting point. This area will be explored in further research. Another topic to be discussed is how to interpret the legal requirements defined in the articles and recitals. Lawyers and court rulings will argument about certain formulations in the GDPR. Therefore, we advise to include legal experts in the requirements engineering process in order to check which requirements apply and whether further requirements from certain legal constellations (e.g. national laws) or changes emerge. Thus, another limitation of this work lies in the probable incompleteness of the list of requirements.

7 Conclusion and Future Work

We present a first proposal of generic reusable technical requirements for the software development process that satisfy the key principles of the GDPR. The requirements can be traced back to the corresponding articles and recitals, thus, making regulatory compliance demonstrable. Furthermore, we link those requirements to stakeholder interests. As a result, we need to consider stakeholder interests with regard to security properties as well as privacy properties in future research.

As indicated in the discussion, the impact of national laws on the requirements worked out in this research should be assessed as a next step. Furthermore, when considering data transfers to third countries or international organizations outside of the EU, national laws of these countries must be taken into account. This is an especially interesting topic for a cloud deployment of the software.

In order to demonstrate applicability of our findings, we will apply the requirements to a specific application context. Once all requirements for compliant software in a specific software product are identified, it should be investigated which measures can be implemented and verified using automated mechanisms. This requires, in particular, more research on TOMs and includes, for example, specifying requirements with regard to privacy by default and privacy by design – taking into account privacy-enhancing technologies – as well as security by design.

References

1. AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. von der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (April 2018), `https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode\_V1.1.pdf`, v.1.1, last accessed on 2018-07-13
2. Beckers, K., Faßbender, S., Küster, J.C., et al.: A pattern-based method for identifying and analyzing laws. In: International Working Conference on Requirements Engineering: Foundation for Software Quality. pp. 256–262. Springer (2012)
3. Boardman, R., Mullock, J., Mole, A.: Bird & bird & guide to the general data protection regulation (May 2017), `https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en`, last accessed on 2018-07-13
4. Bräunlich, K., Richter, P., Grimm, R., Roßnagel, A.: Verbindung von CC-Schutzprofilen mit der Methode rechtlicher IT-Gestaltung KORA. Datenschutz und Datensicherheit-DuD **35**(2), 129–135 (2011)
5. Breaux, T.D.: Legal requirements acquisition for the specification of legally compliant information systems. Ph.D. thesis, North Carolina State University (2009), `https://repository.lib.ncsu.edu/bitstream/handle/1840.16/3376/etd.pdf?sequence=1&isAllowed=y`, last accessed on 2018-07-17
6. Cesar, J., Debussche, J.: Novel EU Legal Requirements in Big Data Security: Big Data-Big Security Headaches. J. Intell. Prop. Info. Tech. & Elec. Com. L. **8**, 79–88 (2017)
7. Christian, T.: Security requirements reusability and the square methodology. Tech. rep., Carnegie-Mellon University (Sep 2010), `http://www.dtic.mil/dtic/tr/fulltext/u2/a532572.pdf`, last accessed on 2018-07-17
8. Colesky, M., Hoepman, J.H., Hillen, C.: A critical analysis of privacy design strategies. In: Security and Privacy Workshops (SPW). pp. 33–40. IEEE (2016)
9. Compagna, L., El Khoury, P., Krausová, A., et al.: How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artificial Intelligence and Law **17**(1), 1–30 (Mar 2009)

10. Danezis, G., Domingo-Ferrer, J., et al.: Privacy and Data Protection by Design – from policy to engineering. Tech. rep., ENISA (December 2014), https://arxiv.org/ftp/arxiv/papers/1501/1501.03726.pdf, last accessed on 2018-07-13
11. Diver, L., Schafer, B.: Opening the black box: Petri nets and Privacy by Design. International Review of Law, Computers & Technology **31**(1), 68–90 (2017)
12. European Union: General Data Protection Regulation (GDPR): Articles (2018), https://gdpr-info.eu/, last accessed on 2018-07-13
13. European Union: General Data Protection Regulation (GDPR): Recitals (2018), https://gdpr-info.eu/recitals/, last accessed on 2018-07-13
14. Hammer, V., Roßnagel, A., Pordesch, U.: KORA: Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für IuK-Systeme. provet (1992)
15. Hansen, M.: SDM-Bausteine (July 2018), https://www.datenschutzzentrum.de/sdm/bausteine/, last accessed on 2018-07-13
16. Hoffmann, A., Hoffmann, H., Leimeister, J.M.: Anforderungen an Software Requirement Pattern in der Entwicklung sozio-technischer Systeme. In: Lecture Notes in Informatics. pp. 379–393. Ges. für Informatik (2012), last accessed on 2018-07-17
17. Hoffmann, A., Schulz, T., Hoffmann, H., Jandt, S., Roßnagel, A., Leimeister, J.: Towards the use of software requirement patterns for legal requirements. In: 2nd International Requirements Engineering Efficiency Workshop (REEW) 2012 at REFSQ 2012. SSRN Journal (SSRN Electronic Journal) (2012), Essen, Germany
18. i-SCOOP: GDPR: legal grounds for lawful processing of personal data (July 2018), https://www.i-scoop.eu/gdpr/legal-grounds-lawful-processing-personal-data/, last accessed on 2018-07-13
19. ico.: Guide to the General Data Protection Regulation (GDPR) (March 2018), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, version 1.0.122, last accessed on 2018-07-13
20. Jensen, J., Tøndel, I.A., Jaatun, M.G., Meland, P.H., Andresen, H.: Reusable security requirements for healthcare applications. In: International Conference on Availability, Reliability and Security, 2009. ARES'09. pp. 380–385. IEEE (2009)
21. Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., et al.: Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. Computer Standards & Interfaces **36**(4), 759 – 775 (2014)
22. Otto, P.N., Antón, A.I.: Addressing legal requirements in requirements engineering. In: 15th IEEE International Requirements Engineering Conference, 2007. RE'07. pp. 5–14. IEEE (2007)
23. Ringmann, S.D., Langweg, H.: Determining security requirements for cloud-supported routing of physical goods. In: 2017 IEEE Conference on Communications and Network Security (CNS). pp. 514–521. IEEE (2017)
24. Simić-Draws, D., Neumann, S., et al.: 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 (2013)
25. Toval, A., Olmos, A., Piattini, M.: Legal requirements reuse: a critical success factor for requirements quality and personal data protection. In: Proceedings IEEE Joint International Conference on Requirements Engineering. pp. 95–103 (2002)
26. Toval, A., Nicolás, J., Moros, B., García, F.: Requirements reuse for improving information systems security: A practitioner's approach. Requirements Engineering **6**(4), 205–219 (Jan 2002)
27. Velasco, J.L., Valencia-García, R., Fernández-Breis, J.T., Toval, A., et al.: Modelling reusable security requirements based on an ontology framework. Journal of Research and Practice in Information Technology **41**(2), 119 (2009)