Privacy Control Patterns for Compliant Application of GDPR

Completed Research

Daniel Rösch
Pforzheim University
daniel.roesch@hs-pforzheim.de

Thomas Schuster
Pforzheim University
Thomas.schuster@hs-pforzheim.de

Lukas Waidelich
Pforzheim University
lukas.waidelich@hs-pforzheim.de

Sascha Alpers
Forschungszentrum Informatik
alpers@fzi.de

Abstract

The exchange of sensitive information has become an important part of our daily lives. This does effect business and personal data. Data exchange is subject to legal regulations. Since May 2018, the European Data Protection Regulation (EU-GDPR) has specifically regulated the protection of personal data. The regulations and possible penalties for non-compliance still lead to uncertainty in many companies. This article exposes techniques in which day-to-day work can be designed in conformity with EU-GDPR. Therefore, we define privacy control patterns that transfer existing GDPR requirements into technical solution templates for compliant services. These patterns contain generally applicable guidelines in the sense of data protection and privacy. The catalogue of patterns serves as a book of reference for providers and users of ICT-services to reduce and overcome uncertainties associated with GDPR implementation and compliance. To demonstrate the implementation of our patterns, we introduce the application system EDV.

Keywords

General Data Protection Regulation (GDPR), EU-GDPR, Design Pattern, Privacy Control Pattern, individual information rights.

Origin and Challenges of Today's Data Protection Regulations

Digital transformation is increasingly becoming a pervasive part of our society. Besides the digitalization of traditional business processes, data-driven business models are the result of this change. In order to meet changing requirements, research and development constantly emerge new technologies. In recent years, this has led to the introduction of many new technologies that are particularly suited to generate and process large volumes of data. One of these trends is the Internet of Things, which generates large amounts of data, that arise in the interaction between analogous and digital environments. Through the efficient processing of these data volumes, e.g. using Big or Smart Data technologies, innovative services can be established by companies. In addition, this change is perceived in society and in some cases considered in a critical way. The accumulation of large amounts of data about an individual in combination with data processing can have a negative impact on an individual's privacy. The new regulation aims to protect data in order to protect privacy. Since organizations exchange data with each other via several interfaces and services, an increased need for data protection is necessary (Kurtz et al. 2018). For these reasons, a new GDPR (European Parliament 2018) was established at European level. It became effective on 25th May 2018 (Labadie and Legner 2019). The EU-GDPR aims to improve data protection (protection against data misuse) by forcing new regulations such as privacy by default and privacy by design to proactively design data protection-friendly IT-Systems (Kurtz et al. 2018). However, it is often misunderstood as the protection of data in general and in some cases considered as obstacle to technological advancement. With this article we intend to point out that the new EU-GDPR is a guideline towards modern technology development in respect to data privacy (legally compliant use of data). This is an opportunity for development of technologies with respect to individual citizen rights (Labadie and Legner 2019). Another

benefit can be increased transparency in data processing for everybody, which could create a common understanding of data as a raw material and its value (McAfee et al. 2012). The actual technical challenge is the fulfilment of the EU-GDPR through standardized security technology. Responsible actors processing personal data must take appropriate technical and organizational measures to protect individual rights of affected persons (Burns 2018). Implementation costs, types, scope, conditions and purposes of data processing must be considered carefully. Moreover, risks associated with the processing of personal data need to be taken into account. This includes the estimation of the likelihood of risk occurrence as well as the severity of risks.

In essence, this article aims to improve the understanding of requirements related to EU-GDPR and to provide knowledge for the creation of compliant technical implementations, for example digital services. For this purpose, we define patterns, which describe the requirements and provide technical solution strategies for a compliant implementation. In order to promote the reusability of technical solution approaches, we point out cross-connections between the requirements – for this purpose, we link the patterns with each other accordingly. Our patterns are structured according to a defined schema (problem definition, context, solution approach), as it is known from other research areas (Alexander et al. 1995) and especially from software engineering (Fowler 2003; Gamma and Riehle 2008; Hohpe and Woolf 2004). The patterns serve as blueprints that offer solution strategies for questions that may arise in daily business.

The initial situation and motivation of the work is the question whether it is possible to derive patterns that describe requirements and generalized technical solutions based on the EU-GDPR. With that in mind, we defined the following concrete research questions:

Q1. Is it possible to transform EU-GDPR requirements into solution patterns?
Q2. Based on the patterns, can EU-GDPR compliant technical solutions be designed and implemented?

Design Principles and Basics of Privacy Pattern Construction

The GDPR describes several principles for the processing of personal data. These include Lawfulness, Fairness, Transparency and Traceability, Purpose Limitation, Data Minimization, Accuracy, Storage Limitation, Integrity and Confidentiality and Accountability (Article 5). Some of the principles cannot be fulfilled by technical measures or the implementation is very time-consuming. These include Lawfulness, Fairness, integrity and confidentiality and accountability. In particular, the principle of Lawfulness processing in good faith (Article 5 (1a), Article 6(1)) GDPR cannot be implemented by any technical measure in general. Lawfulness, which includes the prohibition subject to permission, means that the processing of personal data is generally subject to a prohibition. An exception to this would exist if certain conditions of authorization existed (Article 6 (1)). It is generally complex to assess whether one of the conditions of permission (e.g. a public or legitimate interest) exists. As a result, various individual solutions must be used. However, by recording consents and objections, for example, it is possible to prove at least that the consent was permitted. In contrast, the design and implementation of a system made it easier to comply with the principle of Accountability through explicit and well documented technical measures (Article 5 (2)). The principle of Integrity and Confidentiality cannot be guaranteed by any single technical measure but requires a system-specific catalogue of measures. In this article, we focus on the principles that can be implemented through technical measures with reasonable effort. Thus, the following GDPR principles in particular can be summarized in patterns: Transparency and Traceability (1), Purpose Limitation (2), Data Minimization (3), Accuracy (4) and Storage Limitation (5). The Q1 can already be successfully answered by the formulation of suitable patterns.

The methodology used to describe the patterns always has a common structure. Our approach is based on well-known publications on patterns from other fields. In order to be able to present the patterns optimally for our problems and solutions, we have made some structural adjustments in the pattern specification. Accordingly, we understand a pattern as a blueprint, which provides a generalized solution approach (strategy) for a given problem (and a defined context). This paradigm is known in many disciplines and first became popular in architecture and later in software development (Alexander et al. 1995; Buschmann et al. 1996; Berry 2002; Fowler 2003; Blakley and Heath 2004; Gamma and Riehle 2008; Wilder 2012). Often entire catalogues of patterns are described in a theme-oriented manner. Numerous publications describe further approaches to pattern development (Reiter and Rubin 1998; Romanosky et al. 2006; Schumacher 2003; Schümmer 2004; Steel et al. 2006; Wilder 2012). In the area of security, patterns have already been

identified and described (Blakley and Heath 2004; Steel et al. 2006). Nevertheless, as mentioned earlier, there are only few pattern descriptions in the area privacy. Some other patterns are use-case related. Such as patterns for online transactions as given by Romanowsky (Romanosky et al. 2006). Another example for data protection patterns and considerations is related to online and mobile photo transmission is provided by Ahern et al. (Ahern et al. 2007). We developed our patterns, since no general data privacy pattern catalogue is defined yet. Engels focuses on the law of data portability and works out the accompanying influence on competition dynamics (Engels 2016). Fox et al. concentrates on the principle of transparency by proposing guidelines for compliant privacy notices (Fox et al. 2018). Only Huth and Kurtz consider all GDPRs (Huth 2018; Kurtz et al. 2018). Whereby Kurtz summarizes practical solutions in the context of privacy by design. Since individual authors concentrate only on selected requirements, a broad understanding is missing concerning GDPR and how this can be implemented in enterprises (Burns 2018; Labadie and Legner 2019).

Development and Analysis of Privacy Control Patterns

The development of privacy control patterns is based on the information systems research framework (Hevner et al. 2004). Hence, our development focusses applicable knowledge and for EU-GDPR complaint information system implementation. In this case Hevner's environment aspect includes the EU directives in form of GDPR, which impose solid business requirements. At knowledge base level, we utilize methods for the development of design patterns as known in the field of software engineering (Berry 2002; Blakley and Heath 2004, 2004; Buschmann et al. 1996; Fowler 2003; Gamma and Riehle 2008; Wilder 2012). The design science approach envisages the development of artefacts that are regarded as viable form of a construct. In a first step, GDPR requirements were identified by analysis, which we clustered into several criteria. Thus, explicit requirements could be derived from restrictions defined by GDPR articles. Considering these requirements, we were then able to develop technical solution templates. In combination with checklist-style questions, we created several privacy design patterns. These patterns are outlined below and form a key result (artifact) of the research design. The patterns can find use in the business environment in order to meet the challenge of the conformal use of the GDPR. In addition, this work delivers a benefit in kind of a knowledge base extension. The evaluation process according to the research framework of Hevner et al. consists of several steps. On the one hand, the artifacts were evaluated by workshops with experts, on the other hand, the approach was tested for practicability in the EDV research project.

This article focuses three main areas of privacy, which we derived from EU-GDPR (European Parliament 2018) regulations. These include general privacy control patterns (I), patterns that reflect rights of affected the person, known as the data subject (II) and patterns that reflect obligations of those responsible for services, known as controller and processor (III). Each of our patterns is identified by a unique name. This ensures quick and enhanced access to solution models (pattern strategies) for specific requirements imposed by the EU-GDPR. We strive to address particularly relevant principles and requirements of GDPR in this article. Further GDPR principles can be supplemented later and according the same schema (pattern description). Our patterns are outlined as follows: in the first paragraph (*GDPR requirements*), requirements imposed by EU-GDPR are provided and legislative text is referenced. In the second paragraph (*Resulting challenge*), the problem imposed by these requirements is examined in detail. There is a clear identification of the problem as well as the affected components. In the third part of each pattern (*Technical Solution Approach*), we present techniques to solve the problem. In case of technical options, the reader is free to choose which solution fits best for a given use case. Finally, the last paragraph (*Checklist*) provides a checklist. The checklist allows tracking whether all pattern related GDPR requirements have been met and whether compliance is ensured. Furthermore, dependencies between all patterns are shown in the section Pattern Evaluation. Because of space restrictions we won't provide descriptions of all patterns in this article.

General Privacy Control Patterns (I)

This section embraces central GDPR requirements, which we summarize as generalized privacy control patterns. Altogether, we have derived five patterns in this general part. The following subsections outline the most prevalent of these patterns: Transparency and Traceability (1), Purpose Limitation (2) and Storage Limitation (5).

Transparency and Traceability (1)

GDPR Requirements: personal data shall be processed in a transparent manner that is understandable to the data subject (Article 5 (1a)).

Resulting Challenge: The manner in which a service operates, and all relevant data processed in relation to an individual shall be identified and disclosed. It has to be stressed that disclosure and expulsion are a continuous requirement for the service. The core challenge is therefore to provide an interface that discloses information to the data subject, to fulfill transparency and traceability as required.

Technical Solution Approach: Three technical aspects have to be taken into account in order to meet the requirements of transparency and traceability:

1. *Overview of collected data*: even before using the service, the provider must deliver a list of all data that is possibly collected by a service. For this aspect, the technical solution approach of Information Obligation (6) is recommended for implementation.
2. *Disclosure of stored data*: Refer to the technical solution of the pattern Right of Access.
3. *Disclosure of data processing*: this aspect is the utmost challenge. Ideally, all cloud processes relevant to the data subject should be disclosed in a transparent manner. In addition to the privacy statement, the disclosure of code (open source) can provide technically perceptive individuals with a deeper understanding of the way data is processed. At the very least, however, the provider should answer the key questions of the following checklist before collecting the data.

Checklist:

- Have the questions of the checklist Information Obligation (6) been answered?
- Does the declaration of service contain procedures for processing of personal data?
- Is an explanation provided, that describes how collected data is handled and how a possible transfer of the data (to third parties) is handled?

Purpose Limitation (2)

GDPR Requirements: Personal data must only be collected for specified, explicit and legitimate purposes and may not be further processed in an incompatible manner. Further processing for archival purposes of public interest, for scientific or historical research purposes or for statistical purposes (Article 89 (1)) must not be considered incompatible with the original purposes (Article 5 (1b)).

Resulting Challenge: Processing purposes must be clearly identifiable from data protection declaration. Data may only be accessible for the processing operations that are necessary for the stated purpose.

Technical Solution Approach: Provision of a statement describing the purposes of personal data processing. In addition, two cases must be distinguished for the service implementation.

1. *Data is stored centrally:* We recommend to logically divide processes according to processing purposes (business capability). The data is stored together with the declared purpose. This enables access control of the processing processes to the stored data with the processing purpose as access policy.
2. *Each process stores data (decentralized):* This includes that each service component stores data independently and redundantly. The processing of data must remain clearly assigned to purposes.

Checklist:

- Are clear and legitimate processing purposes established?
- Does the privacy statement describe all processing purposes?
- Are processing operations (service components) divided into processing purposes?
- Is stored data explicitly assigned with purpose attributes? Is data exclusively stored for a specific purpose in isolated processing components (operations)?

Storage Limitation (5)

GDPR Requirements: Personal data must be stored in a form, which permits identification of the data subjects only as long as it is necessary for the purposes for which they are processed (Article. 5 (1e)).

Resulting Challenge: The storage duration of personal data must be defined. In fulfilling the purpose, personal data must be removed from the system or the link to the personal data must be removed in such a way that the identification of the data subject is no longer possible. This is particularly difficult to achieve.

Technical Solution Approach: The data model must include a data lifecycle. The lifecycle is based on time and attributes that declare a processing purpose. If the data is encrypted, an irreversible deletion of the key is sufficient to make the data non-identifiable. Other anonymization mechanisms, such as Differential Privacy (Dwork 2008) are possible, but extremely difficult to implement in practice.

Checklist:

- Is the data associated with a limited storage period (due to a specific purpose)?
- If anonymization is required: Is an appropriate anonymization mechanism in use to safe the stored data?
- If the data is encrypted: Is it possible to delete the encryption key irreversibly?

Data Subject Rights Patterns (II)

In addition to general EU-GDPR requirements, patterns that reflect the rights of affected persons are listed and described in this section. These include the Information Obligation (6), the Right of Access by the Data Subject (7), the Right to Rectification (8), the Right to Erasure (9), the Right to Restriction of Processing (10) and the Right to Data Portability (11). As in the previous section, we explain the main patterns.

Information Obligation (6)

GDPR Requirements: At the time of the collection of personal data, all information must be communicated to the data subject (Article 13 (1), (2)).

Resulting Challenge: According to the EU-GDPR guidelines, the information must be understandable, easily accessible and communicated in clear and simple language in a written or electronic declaration to the data subject. However, awareness of the privacy statement must be a mandatory requirement for successful use of digital services. In addition, the data protection declaration must always be (even after the information has been provided) and easy to find (through max. 2 steps).

Technical Solution Approach: The data protection declaration must be shown to the affected person as text/image symbols in the application before the user registers. The subsequent registration may only be possible after the successful knowledge of the data protection declaration has been recorded. During use, the data protection declaration must be easy to find in the user interface at any time.

Checklist:

- Does the notification provide the following information: Name, contact details of the person responsible for data collection, contact details of the data protection officer, purposes of data processing and their legal basis, recipient of personal data, intention to transfer to a third country, duration of storage, right of access, rectification, deletion, limitation, revocation and complaint to a regulatory authority?
- Provision of personal data required by law or by contract?
- Do you use profiling? If so, notification of logic and implications involved?
- Is the data protection declaration easy to understand and easy to find at any time?

Right of Access by the Data Subject (7)

GDPR Requirements: The data subject has a right of access to the following information: Processing purposes, categories of personal data, recipients or categories of recipients (third countries, organizations), planned storage time, right of rectification and erasure, right of appeal, origin of the data if the personal data was not directly collected, automated decision making including profiling (Article 15, (1)), safeguards in the case of data transfer to a third country (Article 15 (2)), copies of the personal data (Article 15(3)).

Resulting Challenge: Data subjects can make use of a request for information. The person responsible must be able to answer this request in written or electronic form. In this case, the person responsible must use all reasonable means to verify the identity of the data subject seeking information. If there are

reasonable reasons to doubt the identity, the person responsible may request additional information. If the data subject cannot be identified, the person responsible may refuse to provide the information.

Technical Solution Approach: In order to support this challenge technically, flexible interfaces are necessary, which make it possible to request data from the system. For example, Representational State Transfer (REST) interfaces or other interface solutions could be used to retrieve data from the system explicitly. Accordingly, standard queries must be defined that extract relevant information (see EU-GDPR specification) from the backend. The information must then be identified to the user in the front-end by means of text and, if necessary, images. If the user only wishes to obtain specific information, selection functions must be provided. Depending on the selection, only the corresponding information is provided.

Checklist:

- Does the system provide a way to obtain information about a person and the data related to that person?
- Does the system include mechanisms to authenticate clients (person) which request information?

Right to Erasure (9)

GDPR Requirements: A user may request the deletion of personal data concerning him or her. The data controller is obliged to delete data, if the request is justified (Article 15 (1 a-f)). This includes the revocation of consent. The request for deletion shall be forwarded to other affected data controllers as well (Article 15 (2)). Furthermore, some case define exceptions to this rule (Article 15 (3)).

Resulting Challenge: The EU-GDPR requires a function to erase personal data. Accordingly, the user must be able to order the erasure of his data. It must be ensured that the deletion can be forwarded to other responsible parties.

Technical Solution Approach: Similar to the pattern right to Information Obligation / Right of Access by the Data Subject, an interface must be provided which enables the subsequent erasure of personal data. Data of individual persons must be retrievable and separately erasable. Subsequent reproduction of the data after deletion is not permitted.

Checklist:

- Does the system allow the erasure of user data and accounts?

Right to Restriction of Processing (10)

GDPR Requirements: Under certain conditions (Article 18 (1)), the data subject has the right to request limited data processing from the data processors.

Resulting Challenge: The following challenges can be derived from the three paragraphs of the article (Article 18):

1. Each process must be isolated from the others so that the restriction has no impact on other processes.
2. Restrictions applied to a process must not lead to the deletion of data. Hence, separation of data and processes has to be applied as consequently as needed.
3. The processing must be resuscitable.

Technical Solution Approach: A microservice architecture tailored to the specific use-case tackles all three challenges. In particular, the data service (usually a database) must be isolated from others. With the help of a fine-granular microservice architecture, processing components can be isolated from each other. This allows to restrict processing. If it is not possible to implement a microservice architecture, it is advisable to encapsulate the processes using standardized interfaces (e.g. REST). Each processing component should have its own separate interface. Data is stored isolated in separate databases (Alpers et al. 2015). By means of user access control, restricted processing can be enacted.

Checklist:

- Is stopping of a single service free of side effects (for other services)?
- Is each service component (process) encapsulated by an API?
- Is the database independent of the services?

- Can a service component (process) recover its previous state and continue processing as expected?
- Is there a user access control to restrict processing?

Right to Data Portability (11)

GDPR Requirements: If the data processing is automated based on a consent or a contract, the data subject has the right to obtain personal data concerning him/her in a structured, common and machine-readable format. The data subject may communicate this data to other data processors (Article 20 (1)).

Resulting Challenge: The following challenges can be derived from the four paragraphs of the article (Article 20).

1. The requested data must be provided in a structured, common and machine-readable format. Ideally, a selection of common formats should be provided.
2. Data query interfaces shall be provided to other responsible persons. These interfaces may only be opened for other responsible persons on behalf of the person concerned.

Technical Solution Approach: A download form with a selection of exchange formats (e.g. XML, CSV or JSON) is available. In addition, it is possible to open the data service in various formats for other data processors. This allows the data to be exchanged automatically on behalf of the data subject. For this purpose, a secure authorization procedure must be used (e.g. SAML, oAuth). For a successful exchange, the documentation of the interface must be provided.

Checklist:

- Are the exchange formats used common and documented?
- Does the data service offer interfaces for automatic data exchange with other responsible parties and are these interfaces documented?
- Is the interface equipped with a suitable authorization?

Controller and Processor Obligation Patterns (III)

As a third area of privacy requirements, GDPR stipulates various obligations for parties in control of data. These include the Notification Obligation (12) and Privacy by Default (13), which both optimize data privacy protection. We will only outline the second pattern in this section.

Privacy by Default (13)

GDPR Requirements: Appropriate technical and organizational measures shall be taken to ensure that the default settings of a service do not patronize users in the collection, processing, storage and disclosure of personal data. This is often referred to as Privacy by Default (Article 25 (2)).

Resulting Challenge: First, it is necessary that the collection, processing, storage and transfer of data can be technically adjusted to any relevant user context. Only then variable data privacy-friendly default settings are possible.

Technical Solution Approach: In the General pattern section, we have recommended to associate data with additional attributes (e.g., the "purpose limitation" pattern suggests to store an additional "purpose" attribute with personal data). Thus, an attribute-based access control can technically guarantee purpose limitation. If data is provided with proper attributes, then it is technically possible to define data protection-friendly characteristics of these attributes. Thus, data can be provided with the generic storage attribute “by default”, so that no processing process can access these attributes, since they are initially only intended for storage. The same is possible with the time attribute, which determines a lifetime depending on the type of date; once this has expired, further processing can no longer take place. The attribute should be set individually by the person concerned. The two attributes are only examples. The operator of a service must already consider the requirements of this pattern during the design of the data model and define suitable attributes together with their specifications.

Checklist:

- Does the system have suitable control attributes that identify the data?

- Can users flexibly adjust settings regarding the processing of personal data?
- Are users not patronized by the system?

Pattern Evaluation

Derived from the pattern description and the previous analysis, we identified dependencies between the 13 patterns. The dependencies are shown graphically in Table 1. The pattern Transparency and Traceability (1) reveals a high dependency. The pattern has relationships to the patterns Purpose Limitation (2), Data Minimization (3), Accuracy (4), Information Obligation (6), Right of Access by the Data Subject (7), Right to Data Portability (11) and Notification Obligation (12).

Main Areas		I					II						III	
	Patterns	1	2	3	4	5	6	7	8	9	10	11	12	13
I	1	-	x	x	x		x	x				x	x	
	2	x	-			x	x						x	x
	3	x		-		x								x
	4	x			-				x	x				
	5		x	x		-								x
II	6	x	x				-	x				x	x	
	7	x					x	-	x	x		x	x	
	8				x			x	-	x	x		x	
	9				x			x	x	-	x		x	
	10								x	x	-			
	11	x					x	x				-	x	
III	12	x	x				x	x	x	x		x	-	
	13		x	x		x								-

Table 1: Dependencies Between Patterns (I= General Privacy Control Patterns, II=Data Subject Rights Patterns, III= Controller and Processor Obligation Patterns)

Considering the patterns, a high degree of interdependence between the individual GDPR articles can be determined in reverse. The common implementation of individual technical measures is recommended. With the presentation of pattern-based technical solutions to ensure compliance with the GDPR, we created a partially solution for research question Q2. For the implementation of the technical solution approaches, the checklists offer a problem-related and goal-oriented assistance. Having said this, we addressed Q2.

Exemplified Application within Project EDV

We evaluated the applicability of selected patterns in a data protection-sensitive research project "Einfaches Digitales Vergessen" (EDV). The EDV project provides a solution approach that considers the principles of the EU-GDPR, the rights of affected person as well as obligations of those responsible for services. The EDV system enables the exchange of documents, whereby access rights and access periods can be specifically defined. For the patterns developed previously, the solution approach of the EDV project is presented.

Transparency and Traceability (1): A data protection declaration is shown before the EDV system is being used. Collected personal data will be listed and reported to the user. In addition, the technologies used as well as the processing method are described. This information can always be requested in the client.

Purpose Limitation (2): The computer system indicates processing purposes in the Data Protection Declaration. Additional to the collected data processing purposes are stored. Thus, the purpose limitation can be evidenced retroactively.

Data Minimization (3): EDV only stores data that is necessary for the document exchange. The system allows you to edit the attributes any time. The docker containers support flexible structural adjustments.

Storage Limitation (5): Personal data is stored encrypted in the system. Due to a processing time, the related documents can only be viewed for a defined period. After the expiry of this period, the documents are deleted and are no longer accessible. The sender (owner of the data) can change the deadlines.

Information Obligation (6): Before using the EDV system, the user is informed who is processing the data and which data is being processed and stored. The user is also informed of his or her rights.

Right of Access by the Data Subject (7): The user has the possibility to request information about his data at any time. On request the user receives all relevant information concerning the user. In addition, the user can view in the EDV application which data in the system are stored at which time.

Right of Erasure (9) / Restriction of Processing (10) / Data Portability (11): The user has full control over his documents via EDV, so that the user can correct previous information. This results in a reduction of the access time or the withdrawal of reading or writing rights to a document. If personal data is changed or corrected, a notification is sent to the affected person.

Privacy by Default (13): The EDV system offers user-friendly data protection settings from the very beginning. E.g. the user profile is initially created as private. This means that this profile is not visible to the public. The user can decide freely within the settings whether the profile should be open to the public.

Conclusion and Outlook

In conclusion, it is possible to provide problem-oriented and pattern-based solutions to technical requirements arising within the framework of the EU-GDPR (Q1). As explained before, the patterns deliver a body of knowledge that is applicable to different use cases and information systems. The patterns possess a consistent structure. Based on content, we could classify all patterns into three categories: 1) generally derived from the GDPR; 2) associated to the rights of the affected person, and 3) owed to the duties of the responsible service providers. Thus, the catalogue of patterns can be regarded as set of guidelines to implement GDPR compliant information systems. The application in the EDV system also demonstrates how and to which extent the patterns served to create GDPR compliance. We believe that the patterns are eligible to equalize current uncertainties regarding the GDPR regulations. Altogether, we could derive 13 patterns in a first catalogue. Due to the legal regulations, we identified 13 dependencies between these patterns – described in the pattern evaluation. In each pattern, challenges and technical solution approaches are pointed out (Q2). To simplify pattern implementation, we have integrated checklists into the descriptions. This enables users to implement technical services in compliance with legislation.

As already mentioned at the beginning of this article, digitalization will continue to progress. Therefore, data protection and data security will play an increasingly important role in our daily lives. For this reason, it is essential that we continue to take a critical look at this issue. We therefore see the need to describe further requirements from the GDPR explicitly and to develop more pattern-based solution approaches. Although the checklists described above already point in this direction, we plan to support a further simplified application of the patterns (extend Q2). For this purpose, we plan to develop a web-based application that provides an interactive pattern catalogue. The idea would be to enable companies and users to recognize GPDR-based requirements and solution approaches automatically based on their use cases (systems). This could help users to implement and check GDPR compliance. A further future research field is the identification of general data protection patterns, which describe solution strategies independently of legal specifications. This could lead to an extension of our pattern catalogue. Such an extended catalogue might embrace general and law specific patterns, which users could search and filter for certain concepts or laws. As one of the next steps, we plan to investigate this area more closely in order to identify further data protection patterns.

Acknowledgements

This work was supported by the EDV project (Grant No 01MT17009A) funded by the German Federal Ministry for Economic Affairs and Energy within the SmartData funding line.

REFERENCES

Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M., and Nair, R. 2007. "Over-Exposed?: Privacy Patterns and Considerations in Online and Mobile Photo Sharing," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*, San Jose, California, USA: ACM Press, pp. 357–367.

Alexander, C., Ishikawa, S., Silverstein, M., Czech, H., Jacobson, M., and King, I. F. 1995. *Eine Muster-Sprache: Städte, Gebäude, Konstruktion*, Wien: Löcker.

Alpers, S., Becker, C., Oberweis, A., and Schuster, T. 2015. "Microservice Based Tool Support for Business Process Modelling," in *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop*, Adelaide, September, pp. 71–78. (https://doi.org/10.1109/EDOCW.2015.32).

Berry, C. A. (ed.). 2002. *J2EE Design Patterns Applied: Real World Development with Pattern Frameworks*, Birmingham: Wrox.

Blakley, B., and Heath, C. 2004. *Security Design Patterns*, U.K.: The Open Group.

Burns, A. J. 2018. "Security Organizing: A Framework for Organizational Information Security Mindfulness," *The Data Base for Advances in Information Systems* (in Press), pp. 1–17.

Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., and Stal, M. 1996. *Pattern-Oriented Software Architecture: A System of Patterns*, Chichester, NY: Wiley.

Dwork, C. 2008. "Differential Privacy: A Survey of Results," in *Theory and Applications of Models of Computation* (Vol. 4978), M. Agrawal, D. Du, Z. Duan, and A. Li (eds.), Berlin: Springer, pp. 1–19.

Engels, B. 2016. "Data Portability among Online Platforms," *Internet Policy Review* (5:2). (https://doi.org/10.14763/2016.2.408).

European Parliament. 2018. *Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, pp. 1–88.

Fowler, M. 2003. *Patterns of Enterprise Application Architecture*, The Addison-Wesley Signature Series, Boston: Addison-Wesley.

Fox, G., Tonge, C., Lynn, T., and Mooney, J. 2018. "Communicating Compliance. Developing a GDPR Privacy Label," in *Twenty-Fourth Americas Conference on Information Systems*, New Orleans, LA: AISeL, pp. 1–5.

Gamma, E., and Riehle, D. (eds.). 2008. *Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software*, (Nachdr.), Professionelle Softwareentwicklung, München: Addison-Wesley.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75–105.

Hohpe, G., and Woolf, B. 2004. *Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions*, The Addison-Wesley Signature Series, Boston, MA: Addison-Wesley.

Huth, D. 2018. *A Pattern Catalog for GDPR Compliant Data Protection*, pp. 1–7.

Kurtz, C., Semmann, M., and Böhmann, T. 2018. "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors," in *Twenty-Fourth Americas Conference on Information Systems*, New Orleans, LA: AISeL, pp. 1–10.

Labadie, C., and Legner, C. 2019. "Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR," in *14. Internationale Tagung Wirtschaftsinformatik*, Siegen, pp. 1292–1306.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., and Barton, D. 2012. "Big Data: The Management Revolution," *Harvard Business Review* (90:10), pp. 60–68.

Reiter, M. K., and Rubin, A. D. 1998. "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security* (1:1), pp. 66–92. (https://doi.org/10.1145/290163.290168).

Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F., and Friedman, B. 2006. "Privacy Patterns for Online Interactions," in *Proceedings of the 2006 Conference on Pattern Languages of Programs - PLoP '06*, Portland, Oregon: ACM Press, pp. 1–15. (https://doi.org/10.1145/1415472.1415486).

Schumacher, M. 2003. *Security Patterns and Security Standards. With Selected Security Patterns for Anonymity and Privacy*, Thesis, Darmstadt: Darmstadt University of Technology.

Schümmer, T. 2004. *The Public Privacy. Patterns for Filtering Personal Information in Collaborative Systems*, Thesis, Hagen: University of Hagen.

Steel, C., Nagappan, R., and Lai, R. 2006. *Core Security Patterns: Best Practices and Strategies for J2EE, Web Services, and Identity Management*, Upper Saddle River, NJ: Prentice Hall PTR.

Wilder, B. 2012. *Cloud Architecture Patterns. Develop Cloud-Native Applications*, Beijing: O'Reilly.