information

MDPI

Article

Computer-Aided Identification and Validation of Intervenability Requirements

Rene Meis * and Maritta Heisel

paluno – The Ruhr Institute for Software Technology, University of Duisburg-Essen, Duisburg 47057, Germany; maritta.heisel@uni-due.de

* Correspondence: rene.meis@uni-due.de; Tel.: +49-203-379-4503

Academic Editors: Steven Furnell, Sokratis K. Katsikas and Costas Lambrinoudakis

Received: 15 December 2016; Accepted: 6 March 2017; Published: 9 March 2017

Abstract: Privacy as a software quality is becoming more important these days and should not be underestimated during the development of software that processes personal data. The privacy goal of intervenability, in contrast to unlinkability (including anonymity and pseudonymity), has so far received little attention in research. Intervenability aims for the empowerment of end-users by keeping their personal data and how it is processed by the software system under their control. Several surveys have pointed out that the lack of intervenability options is a central privacy concern of end-users. In this paper, we systematically assess the privacy goal of intervenability and set up a software requirements taxonomy that relates the identified intervenability requirements with a taxonomy of transparency requirements. Furthermore, we provide a tool-supported method to identify intervenability requirements from the functional requirements of a software system. This tool-supported method provides the means to elicit and validate intervenability requirements in a computer-aided way. Our combined taxonomy of intervenability and transparency requirements gives a detailed view on the privacy goal of intervenability and its relation to transparency. We validated the completeness of our taxonomy by comparing it to the relevant literature that we derived based on a systematic literature review. The proposed method for the identification of intervenability requirements shall support requirements engineers to elicit and document intervenability requirements in compliance with the EU General Data Protection Regulation.

Keywords: privacy; privacy requirements; intervenability; privacy analysis; requirements engineering; computer-aided software engineering

1. Introduction

A central concern of end-users with regard to privacy is that they have almost no control over their personal data once these are put into an information system [1–4]. End-users wish for more empowerment, i.e., they want to keep control of their personal data and how their data is processed by information systems. Hansen [5] summarizes this and other privacy needs into the privacy goal of *intervenability*. Hansen states *"Intervenability aims at the possibility for parties involved in any privacy-relevant data processing to interfere with the ongoing or planned data processing. The objective of intervenability is the application of corrective measures and counterbalances where necessary."* [5]

Intervenability is a complex software quality that is strongly coupled with other privacy-related goals. For example, end-users have to be sufficiently aware of how and what personal data is processed and which options exist to intervene in order to be able to exercise these options. Hence, the privacy goal of transparency can be seen as a prerequisite for intervenability.

This paper is an extended version of [6]. In [6], we introduced a requirements taxonomy that refines intervenability into subrequirements enriched with attributes and associated to transparency requirements that we identified in [7] as a first step to assist requirements engineers to deal with the

complex privacy goal of intervenability. In this paper, we additionally extend the problem-based privacy analysis (ProPAn) method for the computer-aided identification and validation of privacy requirements [8] with the intervenability requirements identified in this paper. We provide computer assistance by means of a software tool that supports the semi-automatic identification and validation of intervenability requirements. In summary, this paper provides a deeper understanding of the privacy goal of intervenability and its relation to transparency and a tool-supported method that supports the process of the identification and validation of intervenability requirements.

The rest of the paper is structured as follows. The taxonomy of our privacy requirements is derived and presented in Section 2. In Section 3, we then compare this taxonomy to related work that we identified using a systematic literature review. These two sections are originally introduced in [6]. The ProPAn method [8] is introduced in Section 4 as background. The novel contribution of this paper, namely the extension of the ProPAn method to also consider intervenability requirements, is presented in Section 5. Section 6 finally concludes the paper.

2. Deriving and Structuring Requirements on Intervenability

In Section 2.1, we systematically analyze the privacy principles described by the international standard ISO/IEC 29100:2011 [9] and the EU General Data Protection Regulation [10] to derive the intervenability requirements they contain and the transparency requirements related to them. To derive the requirements, we analyze the description of the privacy principles and the formulations of the regulation. We keep the formulation of the identified intervenability and transparency requirements close to the original documents from which we identified them. In Section 2.1, we enumerate these derived requirements using the notation I*n* for intervenability requirements and T*n* for the related transparency requirements. As the ISO principles and EU articles partly overlap, we identified several refinements of identified requirements. We relate those requirements using a *refines* relation. If an intervenability requirement In_1 refines a part of another requirement In_2, this means that In_1 adds further details on how or which possibilities have to exist to intervene in the processing of personal data. Furthermore, we identified that there are transparency requirements that are closely related to intervenability requirements. These transparency requirements state that data subjects have to be aware of the intervenability mechanisms that they can exercise in order to make use of them. Hence, we use a *relatedTo* relation to make the relations between transparency and intervenability requirements explicit. The *refines* (directed dashed edges) and *relatedTo* (solid edges) relation are visualized as an initial overview of intervenability requirements in Figure 1. In Section 2.2, we structure the intervenability requirements identified in Section 2.1 into a taxonomy of intervenability requirements and integrate this taxonomy into the taxonomy of transparency requirements introduced in [7]. The taxonomy is presented as an extensible metamodel using a UML (Unified Modeling Language) class diagram.

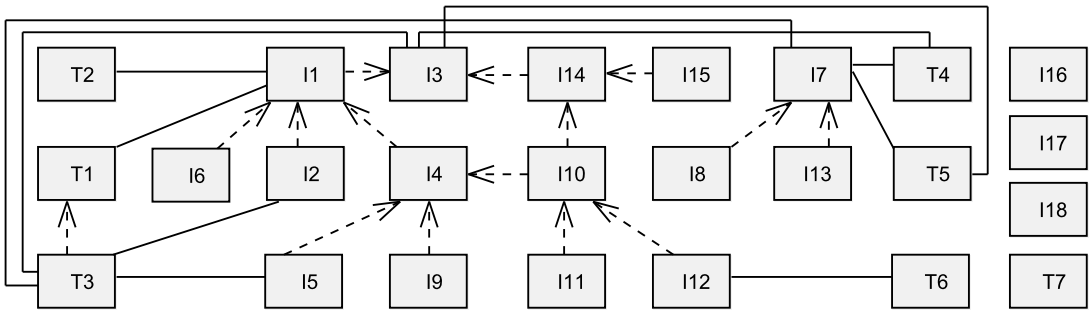

Figure 1. Initial overview of intervenability requirements (taken from [6]).

ISO/IEC 29100:2011 and the EU General Data Protection Regulation do not use the same terminology. To avoid ambiguities, we use the following term definitions from the EU General Data Protection Regulation in this paper.

Personal data *"means any information relating to an identified or identifiable natural person ('data subject')"* This term is called *personally identifiable information (PII)* in ISO/IEC 29100:2011.

Data subject *"An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, on online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."* This term is called *PII principal* in ISO/IEC 29100:2011.

Processing *"means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction."*

Controller *"means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; [...]."* This term is called *PII controller* in ISO/IEC 29100:2011.

Supervisory authority *"means a public authority which is established by a Member State pursuant to Article 51."* Article 51 states that supervisory authorities are *"responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."*

2.1. Requirements Identification from Privacy Principles and Legislation

2.1.1. ISO/IEC 29100 Privacy Principles

To derive our taxonomy of intervenability requirements, we first consider the international standard ISO/IEC 29100:2011 [9], which defines 11 privacy principles which are a superset of the OECD (Organisation for Economic Co-operation and Development) principles [11] and the US fair information practices (FIPs) [12].

We start our analysis with the *consent and choice principle*, which is obviously concerned with providing data subjects the power to decide how their data is processed. From this principle, we obtain the following intervenability and transparency requirements.

- I1 Present the data subjects with the choice of whether or not to allow the processing of their personal data.
- I2 Obtain the opt-in consent of the data subject for collecting or otherwise processing sensitive personal data.
- T1 Inform data subjects before obtaining consent about their rights to access their personal data and to influence the processing of these.
- I3 Provide data subjects with the opportunity to choose how their personal data is handled.
- I4 Allow data subjects to withdraw consent easily and free of charge.
- T2 Where the personal data processing is not based on consent but instead on another legal basis, the data subject should be notified wherever possible.
- I5 Where the data subject has the ability to withdraw consent and has chosen to do so, these personal data should be exempted from processing for any purpose not legally mandated.
- I6 Provide data subjects with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their personal data at the time of collection, first use or as soon as practicable thereafter.

Requirement I3 states that data subjects shall have the opportunity to choose how their data is handled and is the most general intervenability requirement. It is refined by I1 (cf. Figure 1) that states that data subjects shall have the choice whether their data is processed or not. I1 is further refined by I2 that requires opt-in consent for processing of sensitive personal data, I4 that requires the possibility to withdraw consent, and I6 that describes requirements for the mechanisms to realize I1. I5 refines I4 by describing the effects of withdrawing consent. Both transparency requirements T1 and T2 are related to I1 (cf. Figure 1). T1 requires that data subjects have to be informed about their rights before

consent is obtained. T2 requires data subjects to be informed if their data is processed without their explicit consent.

From the *openness, transparency and notice principle* we identify an additional transparency requirement that is related to all intervenability requirements that describe the choices and means for data subjects to influence how their data is processed (cf. Figure 1).

T3 Disclose the choices and means offered by the controller to data subjects for the purposes of limiting the processing of, and for accessing, correcting and removing their information.

The following two intervenability requirements are derived from the *individual participation and access principle*.

I7 Give data subjects the ability to access and review their personal data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law.

I8 Allow data subjects to challenge the accuracy and completeness of their personal data and have it amended, corrected or removed as appropriate and possible in the specific context.

I7 and I8 are not refinements of the already identified intervenability requirements, because they are not concerned with how data subjects can influence how or if their personal data is processed. However, we consider I8 as a kind of refinement of I7, because I8 depends on I7. Note that I7 prescribes that data subjects shall be empowered with the ability to access and review their personal data. Hence, I7 is considered as an intervenability requirement. Nevertheless, allowing data subjects to access and review their personal data also contributes to transparency.

The other principles presented in ISO 29100 do not contain further statements from which we can derive intervenability requirements.

2.1.2. EU General Data Protection Regulation

To identify further intervenability and transparency requirements and to refine the already identified requirements, we analyze the EU General Data Protection Regulation [10]. We selected this regulation as a representative data protection regulation. In contrast to the situation in the US where no privacy regulations covering all industrial branches exist, the EU data protection regulation covers all industrial branches.

Article 7 describes the conditions for consent and we derive from it the following intervenability requirement that refines I4.

I9 The data subject shall have the right to withdraw his or her consent at any time.

Article 12 specifies requirements on mechanisms for exercising the rights of data subjects. We identified the following two transparency requirements that are related to all intervenability requirements that describe the choices and means for data subjects to influence how their data is processed.

T4 The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken if a data subject requested information and shall provide the requested information.

T5 If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Article 15 describes the right of access by the data subject. We do not derive further requirements from Article 15, but it supports the intervenability requirement I7 and transparency requirement T3.

The right to rectification is defined in Article 16. This right is already covered by the intervenability requirement I8.

Article 17 is about the right to be forgotten and to erasure. From this article, we derive the following requirements.

I10 The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data if the data subject withdraws consent or objects to the processing of personal data.
I11 The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary.
I12 Where erasure is not possible, the controller shall instead restrict processing of personal data.
T6 The controller shall inform the data subject before lifting the restriction on processing.

I10, I11, and I12 refine the consequence of withdrawing consent (I4) and objecting to processing (I14 see below). T6 requires that data subjects are informed about the restrictions on processing implied by I12 before these are lifted.

The right to data portability is introduced by Article 20. It implies the following intervenability requirement that refines I7.

I13 The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

Article 18 is about the right to restriction of processing. This right overlaps with the right to object described in Article 21. From these Articles, we derived the following two intervenability requirements that refine I3.

I14 The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data, unless the controller demonstrates compelling legitimate grounds for the processing.
I15 If the objection is valid, the controller shall no longer use or otherwise process the personal data concerned.

Article 53 describes the powers of supervisory authorities. In contrast to the previously identified requirements, the following requirements do not describe intervention possibilities for data subjects or needs to provide information to data subjects, but for/to supervisory authorities.

T7 Supervisory authorities may order the controller to provide any information relevant to the performance of their duties to them.
I16 Supervisory authorities may order the rectification or erasure of all data when they have been processed in breach of the provisions of a regulation.
I17 Supervisory authorities may impose a temporary or definitive ban on processing.
I18 Supervisory authorities may order to suspend data flows to a recipient in a third country or to an international organization.

Table 1 summarizes the ISO 29100 principles and articles of the EU General Data Protection Regulation from which initial intervenability and transparency requirements were derived. Additionally, it allows to associate the elements of our intervenability requirements taxonomy (introduced in the next section) with the principles and articles from which these were identified.

Table 1. Mapping of ISO principles and data protection articles to the requirements.

Principle/Article	I*n*/T*n*	IR	DIR	AIR	PIR	EIR	IIR
Consent and choice	I1-I6, T1, T2	X	X		X		
Openness, transparency and notice	T3		X		X		
Individual participation and access	I7, I8	X	X				
Article 7	I9		X				
Article 12	T4, T5						X
Article 15	I7, T3	X	X		X		
Article 16	I8	X	X				
Article 17	I10-I12, T6	X	X				X
Article 20	I13	X	X				
Article 18 and 21	I14, I15	X	X				
Article 58	I16-I18, T7	X		X		X	

IR: IntervenabilityRequirement **DIR**: DataSubjectInterventionRequirement; **AIR**: AuthorityInterventionRequirement **PIR**: ProcessingInformationRequirement; **EIR**: ExceptionalInformationRequirement **IIR**: InterventionInformationRequirement.

2.2. Setting Up an Intervenability Requirements Taxonomy

We now structure the identified preliminary intervenability requirements into an intervenability requirements taxonomy. We integrate this taxonomy into the transparency requirements taxonomy presented in earlier work [7] using the related preliminary transparency requirements. Figure 2 shows our taxonomy in the form of a metamodel using a UML class diagram. Note that we only show the attributes and enumerations of the transparency taxonomy that are relevant to this paper. All elements that have bold font and thick lines are newly added to the transparency taxonomy. The requirements with dark gray background represent the newly identified transparency and intervenability requirements.

Table 2 provides an overview of how the initial requirements are reflected in our proposed taxonomy. In the following, we explain the new elements of our taxonomy and how they are related to the requirements introduced in [7].

Table 2. Mapping between taxonomy and preliminary requirements.

Requirement	Attribute	I*n*/T*n*
IntervenabilityRequirement	effect	I1, I3, I5, I7, I8, I10-I13, I15-I18
DataSubjectInterventionRequirement	type	I1-I5, I7, I8, I10-I15
	time	I6, I9, I14
	consequences	T1, T3, I6
AuthorityInterventionRequirement	type	I16, I17, I18
ProcessingInformationRequirement	controlOptions	T1, T3, I6
	grounds	T2
ExceptionalInformationRequirement	exceptionalCase	I16, I17, I18, T7
InterventionInformationRequirement		T4, T5, T6

Intervenability Requirement The root element of our intervenability requirements taxonomy is the IntervenabilityRequirement. We modeled it as an abstract class because only its specializations shall be instantiated. It contains the attribute *effect* that describes the consequences of an intervenability requirement. The possible effects are derived from the preliminary requirements I1, I3, I5, I7, I8, I10–I13, and I15–I18, and are summarized in the enumeration *InterventionEffect* (cf. Figure 2). The effects are that data subjects get *access* to their personal data; that their personal data is *not processed*; that the *processing is restricted*; that their personal data is *amended*, *corrected*, or *erased*; that they *receive a copy* of their data; and that *data flows are suspended*. In addition to the effect that an intervenability requirement

shall have, it has a *type* describing how data subjects or supervisory authorities can cause the wanted effects. As these types differ for data subjects and authorities, we added the attribute *type* to the intervenability requirements *DataSubjectInterventionRequirement* (representing intervention possibilities for data subjects) and *AuthorityInterventionRequirement* (representing intervention possibilities for supervisory authorities).

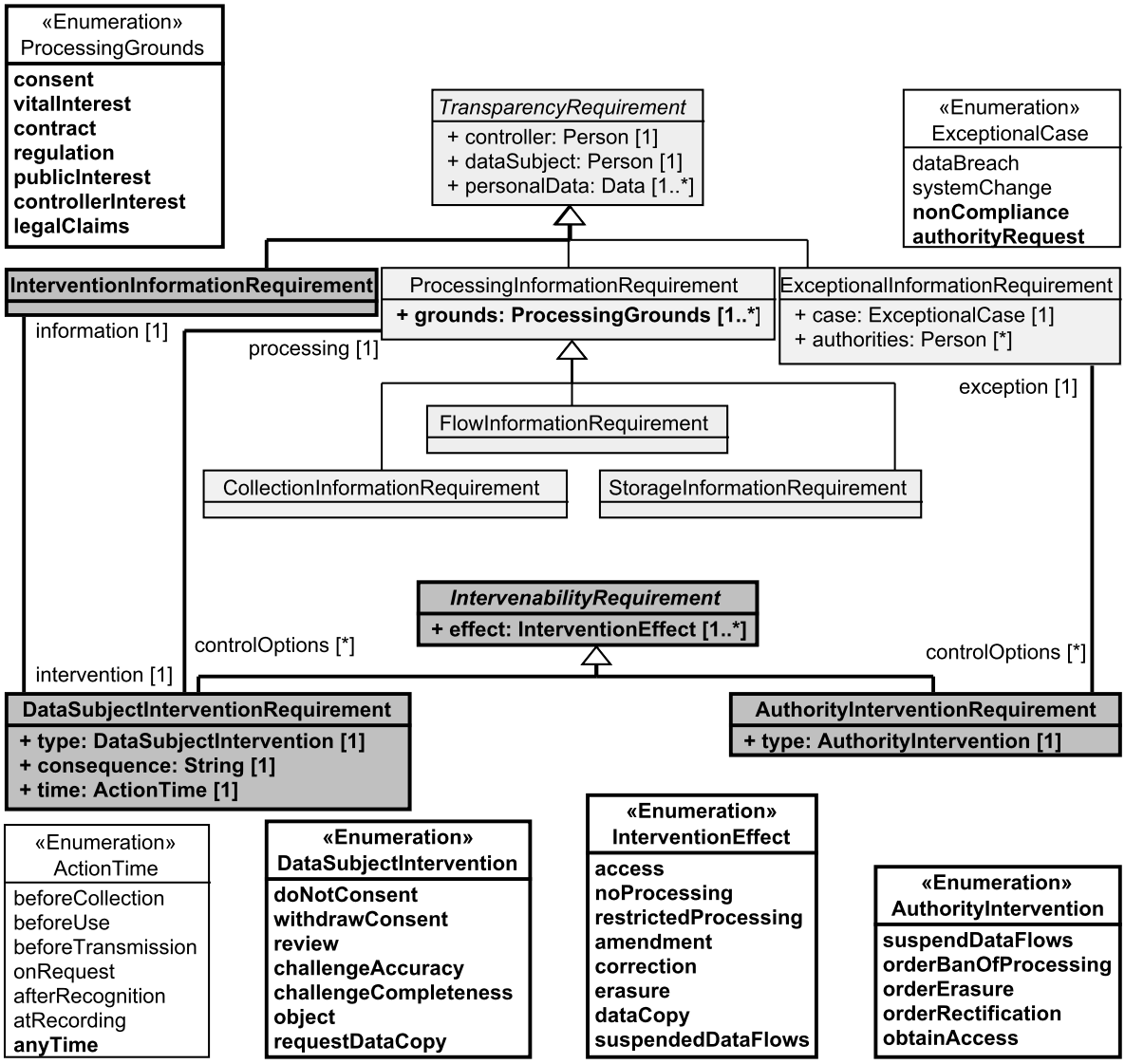

Figure 2. Our combined taxonomy of transparency and intervenability requirements (based on [6]).

AuthorityInterventionRequirement Almost all initial requirements describe rights of data subjects to influence how their personal data is processed. Only I16, I17, I18, and T7 present possibilities for supervisory authorities to intervene in the processing of personal data. The intervention *type*s for authorities are summarized in the enumeration *AuthorityIntervention* (cf. Figure 2). Supervisory authorities may order to *suspend data flows*, order a *ban of processing* of personal data, and order the *erasure* or *rectification* of personal data. The initial requirements I16, I17, and I18 also describe which type of intervention shall lead to which kind of intervention effect. Hence, there are limitations for the combination of intervention types and effects when an *ExceptionalInformationRequirement* is instantiated. Table 3 presents the valid combinations of intervention types and effects.

Table 3. Mapping between authority intervention types and intervention effects.

Intervention Type	Possible Intervention Effects	Source
suspendDataFlows	suspendedDataFlows	I18
orderBanOfProcessing	noProcessing, restrictedProcessing	I17
orderErasure	erasure	I16
orderRectification	correction, amendment	I16
obtainAccess	access	T7

T7 indicates that supervisory authorities have to be informed about the processing in order to exercise their rights to intervention properly. Hence, each *AuthorityInterventionRequirement* has an *ExceptionalInformationRequirement* assigned that describes which supervisory authorities may intervene. We newly introduced into the enumeration *ExceptionalCase* the literals *nonCompliance* and *authorityRequest* to reflect that authorities have to be informed in the case of processing of personal data in a way that does *not comply* with the regulations and that authorities then have the possibility to intervene in this processing. Additionally, authorities have the right to *request* information concerning the processing of personal data from the controller.

DataSubjectInterventionRequirement The *DataSubjectInterventionRequirement* presents the possibilities for data subjects to intervene in the processing of their personal data. These possibilities are summarized in the enumeration *DataSubjectIntervention* (cf. Figure 2) that we derived from the preliminary requirements I1-I5, I7, I8, and I10–I15. These initial requirements additionally describe which combinations of intervention types and effects are allowed for *DataSubjectInterventionRequirements*. The valid combinations are shown in Table 4.

Table 4. Mapping between data subject intervention types and intervention effects.

Intervention Type	Possible Intervention Effects	Source
doNotConsent	noProcessing	I2
withdrawConsent	noProcessing, restrictedProcessing, erasure	I4, I5, I10, I12
review	access	I7
challengeAccuracy	correction, amendment, erasure	I8
challengeCompleteness	amendment, erasure	I8
object	noProcessing, restrictedProcessing, erasure	I10, I12, I15
requestDataCopy	dataCopy	I13

T1, T3, I6, and I9 require that data subjects have to be informed about how they can intervene in the processing of their personal data. To reflect this, we introduced the association *controlOptions* between *DataSubjectInterventionRequirement* and *ProcessingInformationRequirement* (cf. Figure 2). From the perspective of the *ProcessingInformationRequirement*, the association describes which options exist for data subjects to intervene in the processing of their personal data. The two attributes *consequence* and *time* of *DataSubjectInterventionRequirement* are used to describe further details on the control option described by the *DataSubjectInterventionRequirement*. The attribute *consequences* allows providing a textual description of the consequences that the utilization of the corresponding intervenability option has. The attribute *time* describes when data subjects can exercise the corresponding option.

From the preliminary requirements T4–T6, we identified that an additional transparency requirement should be added to the taxonomy. This requirement states the need to inform data subjects about the progress or rejection of interventions requested by them. For this purpose, we introduce the *InterventionInformationRequirement*. Each *DataSubjectInterventionRequirement* is associated to an *InterventionInformationRequirement* and vice versa that presents the need to inform data subjects about the progress or rejection of their intervention.

Furthermore, we identified from T2 that the *ProcessingInformationRequirement* should also inform data subjects about the legal grounds on which their data is processed. For this, we enriched this requirement with an attribute *grounds* that reflects the possible grounds for processing personal data by the controller. These are derived from ISO 29100 and the the EU General Data Protection Regulation. They are *consent* of the data subject, the *vital interest* of the data subject, an existing *contract*, a *regulation* that allows the processing, and *public interest*.

3. Comparison of the Taxonomy with Related Literature

In this section, we give an overview of existing research that also contains considerations about the privacy goal of intervenability. To evaluate our proposed taxonomy, we map the notions and concepts used in the related literature to our taxonomy to check whether it is suitable to reflect the intervenability concepts used in the literature.

To identify the relevant related work, we performed a systematic literature review using backward snowballing [13]. To obtain the starting set of papers for our review, we manually searched the proceedings and issues of the last 10 years of computer science conferences and journals that are mainly concerned with at least one of the topics of privacy, requirements, and software engineering and ranked at least as *B-level* in the CORE2014 [14] ranking. In this way, we selected 15 conferences and 19 journals. First, we checked whether the title or abstract of a paper indicates that the paper is concerned with privacy (requirements), intervenability, empowerment, user's controls, or user's choices. In this way, we obtained 219 articles. We then analyzed the full texts of these articles. Doing this, we reduced the number of relevant articles to 21. Due to the manual search process, we have to deal with the threat to validity that our starting set of papers does not contain all relevant literature, because it was published in a source that we did not consider or was published earlier than in the last 10 years. To mitigate this threat, we applied backward snowballing. That is, we also considered the papers referenced in the papers that we identified as relevant until no new candidates were found. During the snowballing, we identified 79 possibly relevant articles from which 12 were finally considered as relevant. In total, we identified 298 papers that seemed to be relevant after reading the title and abstract. After the analysis of the full text, we finally identified 33 papers as related work. In the following, we provide an overview of our key findings gained from the literature review.

The most important finding is that we are able to map each explicitly mentioned intervenability-related concept in the literature to an element of our taxonomy and that none of the articles provides such a structured overview of intervenability requirements and relates these explicitly to transparency requirements. Table 5 shows to which degree the articles identified during the literature review address the intervenability requirements that we identified in this work. For each article, we investigated to which degree aspects of the *DataSubjectInterventionRequirement* (column **DIR**), the *AuthorityInterventionRequirement* (column **AIR**), and the relations between intervenability and transparency requirements (column **RIT**) are mentioned in it. We distinguish in Table 5 three cases. If all aspects are addressed, we denote this with a "+". If the aspects are only partially considered, then we denote this with a "o". If no aspects are addressed, we denote this with a "-".

Table 5. Mapping of intervenability notions from the literature to our taxonomy.

Source	DIR	AIR	RIT
Bier [15], Hansen [5]	+	+	o
Hoepman [16]	+	o	o
Mouratidis et al. [17]	o	o	o
Miyazaki et al. [18]	+	+	-
Kalloniatis et al. [19,20], Spiekermann and Cranor [21]	o	o	-
Makri and Lambrinoudakis [22], Acquisti et al. [23], Masiello [24], Krol and Preibusch [25], Deng et al. [26], Komanduri et al. [27], Cranor [28], Wicker and Schrader [29]	o	-	o
Strickland and Hunt [30], Sheth et al. [31], Fhom and Bayarou [32], Antón et al. [33,34], Van der Sype and Seigneur [35], Basso et al. [36]	+	-	-
Lobato et al. [37], Caron et al. [38], Zuiderveen Borgesius [39], Breaux [40], Langheinrich [41], Feigenbaum et al. [42], Wright and Raab [43], Guarda and Zannone [44], Hedbom [45], Smith et al. [46]	o	-	-

DIR: DataSubjectInterventionRequirement, **AIR**: AuthorityInterventionRequirement, **RIT**: Relation between intervenability and transparency requirements.

From Table 5, we can see that no article discusses all aspects concerning the relation between intervenability and transparency requirements. Several papers mention that transparency is a prerequisite for intervenability or that data subjects have to be aware of their options to intervene in the processing of their personal data, but none of the papers mentioned that data subjects have to be informed about the progress of the intervention requests that they have triggered. Few of the articles considered the intervention options of supervisory authorities. Only three articles covered all of the aspects and five identified the need to be able to answer requests of supervisory authorities in order to prove compliance with regulations or standards. All articles discuss at least partially options for the data subject to intervene into the processing of their personal data. The most often discussed intervenability option is to consent or withdraw consent. Another interesting observation that we made is that only Hoepman [16] discusses the right to data portability. This right, its implementation, and consequences seem to not yet have been discussed deeply in the literature.

4. Problem-Based Privacy Analysis

In this section, we introduce the problem-based privacy analysis (ProPAn) method, that we extend in the next section to support the intervenability requirements introduced in Section 2. ProPAn is a tool-supported [47] method that supports a privacy analysis of a software system based on its functional requirements represented as problem diagrams [48].

The UML2 activity diagram shown in Figure 3 visualizes the ProPAn method (as described in [8]) to identify and validate privacy requirements based on a set of functional requirements. We will refer to the actions of the activity diagrams using the term *step*. The ProPAn method has to be carried out jointly by a requirements engineer, knowing the functional requirements, a privacy expert, knowing the privacy needs for the system under consideration, and an application domain expert, knowing the application domain of the system under consideration. In the following, we will refer to these persons using the term *user*.

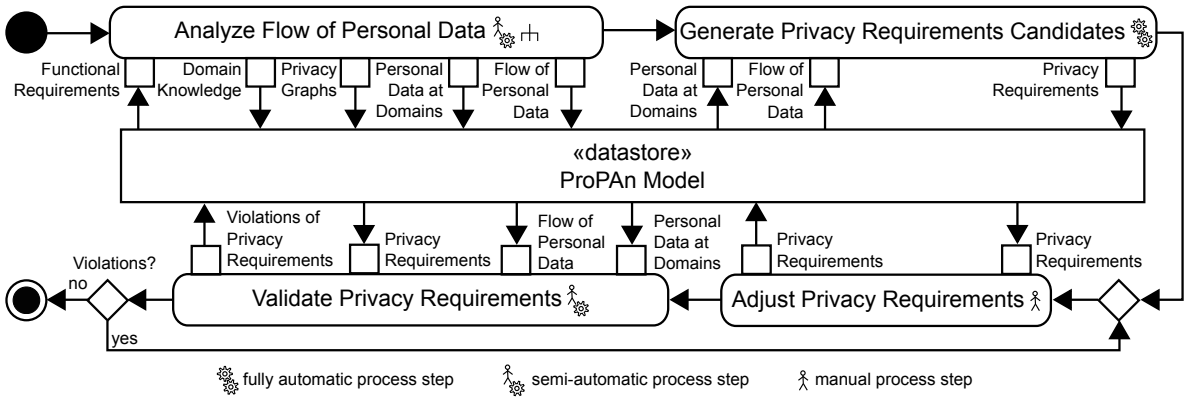

Figure 3. Overview of the ProPAn method [8].

ProPAn builds upon a central UML model, called *ProPAn Model*, which is used to provide the inputs and to store the outputs for all steps of our method. To document all artifacts needed, ProPAn provides an UML profile that defines stereotypes that allow to document a variety of graphs, relations, and privacy requirements used by ProPAn.

In the following, we provide an overview of the four steps of the ProPAn method and briefly describe what is done in the steps and for which purpose, and how the steps are connected to each other. The details on how the steps are carried out can be found in [8].

The first step shown in Figure 3 (*Analyze Flow of Personal Data*) consists of several sub-steps that we presented in previous work. In this step, we identify privacy relevant domain knowledge as introduced in [49,50]; we generate different kinds of graphs that visualize possible privacy issues implied by the functional requirements and the identified domain knowledge as introduced in [51,52]; and we identify the personal data that are processed by the system under consideration, how it flows through the system and at which places (domains) the personal data are available and in which quality it is available there as introduced in [52]. These outputs produced during the first step form the foundation of the following steps.

In the second step of our method (*Generate Privacy Requirements Candidates*), we use the identified *flow of personal data* and the information about the *personal data at domains* to automatically generate the *privacy requirements* that are implied by the provided input. In this paper, we consider the generation of privacy requirements related to the protection goals for privacy engineering proposed by Hansen [5]. These protection goals include the classical security goals *confidentiality*, *integrity*, and *availability* and the privacy goals *unlinkability*, *transparency*, and *intervenability*. The privacy goal of intervenability is not considered in [8]. In this paper, we extend ProPAn to support also the generation and validation of intervenability requirements. Our proposed extension is based on the combined taxonomy of transparency and intervenability requirements that we introduced in Section 2. This means that we generate intervenability requirements based on the transparency requirements that are generated as described in [8], and we link the generated intervenability requirements to their related transparency requirements.

In the third step *Adjust Privacy Requirements*, the user has to review, complete, and adjust the generated *privacy requirements*. This is needed, because the generated privacy requirements may lack details that are not extractable from the ProPAn model or the generated requirements are considered to be incomplete, too strong, or too weak. As a result of this step, we obtain a set of revised privacy requirements.

The revised privacy requirements are validated automatically in the fourth step of our method. It is, for example, checked whether the manually adjusted privacy requirements are still consistent with the flow of personal data and the availability of personal data at the different domains as documented in the ProPAn model. The tool support provides the user information about the kinds of violations of the consistency of the privacy requirements and the elicited information flows. Based on this

information, the user has to decide whether the privacy requirements have to be adjusted again, or whether the presented consistency violations are not violations or acceptable violations.

5. Computer-Aided Generation of Intervenability Requirements

In this section, we show how the steps *Generate Privacy Requirements Candidates*, *Adjust Privacy Requirements*, and *Validate Privacy Requirements* of the ProPAn method (introduced in the previous section) are extended to consider intervenability requirements. Which intervenability options are relevant to a system-to-be depends on the legal framework relevant to the data controller and the data subjects. In this paper, we only consider the case that the controller and the data subjects are all located in the EU. Hence, we generate the intervenability requirements based on the needs to intervene into the processing of personal data implied by the EU General Data Protection Regulation [10]. The extension of the ProPAn method is also integrated into the ProPAn tool [47].

This section is organized as follows. First, we introduce a small eHealth scenario as a running example to illustrate our method in Section 5.1. Then, we describe the extension of the step *Generate Privacy Requirements Candidates* for intervenability requirements in Section 5.2. Section 5.3 explains how the step *Adjust Privacy Requirements* can be performed for intervenability requirements. Finally, we explain how the step *Validate Privacy Requirements* is executed for intervenability requirements in Section 5.4.

5.1. eHealth Application Example

We use a subsystem of an electronic health system (EHS) scenario provided by the industrial partners of the EU project *Network of Excellence (NoE) on Engineering Secure Future Internet Software Services and Systems* (*NESSoS*) [53] to illustrate the proposed method for the identification and validation of intervenability requirements. This scenario is based on the German health care system which uses health insurance schemes for the accounting of treatments.

The EHS is the software to be built. It has to manage electronic health records (EHR) which are created and modified by doctors (functional requirement R1) and can also be browsed by doctors (R2). Additionally, the EHS shall support doctors to perform the accounting of treatments that patients received. The accounting is based on the treatments stored in the health records. Using an insurance application, it is possible to perform the accounting with the respective insurance company of the patient. If the insurance company only partially covers the treatment a patient received, the EHS shall create an invoice (R3). The billing is then handled by a financial application (R4). Furthermore, mobile devices shall be supported by the EHS to send instructions and alarms to patients (R5) and to record vital signs of patients (R6). Finally, the EHS shall provide anonymized medical data to researchers for clinical research (R7).

5.2. Generate Intervenability Requirements Candidates

In this section, we describe how we automatically generate data subject and authority intervention requirements, and exceptional information requirements based on the processing information requirements in the model and the intervention needs described by the EU General Data Protection Regulation.

5.2.1. Data Subject Intervention Requirement

A data subject intervention requirement has the following meaning for the intervention types *doNotConsent*, *withdrawConsent*, *challengeAccuracy*, *challengeCompleteness*, and *object*:

> <*time*> the <*processing.dataSubject*> shall be able to *type* to the processing described in <*processing*>. The intervention shall result in <*effect*> and can have the consequences <*consequence*> for <*processing.dataSubject*>s.

For the intervention types *review* and *requestDataCopy*, we derive the meaning by aggregating all of the data subject intervention requirements with the respective type for each data subject. The meaning is then defined as follows:

> <*time*> the <*processing.dataSubject*> shall be able to *type* (of) his/her personal data <*processing.personalData*>. This action shall result in <*effect*> to/of his/her personal data <*processing.personalData*> and can have the consequences <*consequence*> for <*processing.dataSubject*>s.

In our taxonomy, each data subject intervention requirement is related to a processing information requirement. Hence, the processing information requirements that are generated as described in [8] are the basis for the generation of data subject intervention requirements. To determine which kinds of intervention requirements are needed, we consider the EU General Data Protection Regulation.

The EU General Data Protection Regulation promotes an opt-in scheme for the processing of personal data (cf. Articles 6, 7, and 9). Hence, we add to all processing information requirements *consent* to the documented grounds and generate two intervenability requirements for each processing information requirement. First, we generate one with the intervention type *doNotConsent* and effect *noProcessing*. The time for this intervention requirement depends on the kind of processing information requirement. For collection information requirements, time is set to *beforeCollection*. For flow information requirements, time is set to *beforeCollection* if this information is also directly collected, i.e., a collection information requirement for the corresponding personal data exists, and to *beforeTransmission* if the flowing personal data is not collected by the software, e.g., the personal data is derived from other personal data. For storage information requirements, we distinguish the same two cases. If the stored information was collected by the software, then we set time to *beforeCollection* and else we set time to *atRecording*. Second, we generate a data subject intervention requirement with type *withdrawConsent*, effect *erasure*, and time *anyTime*.

The right of access by the data subject (Article 15) implies that the data subject shall be able to request access to his/her personal data stored by the software or sent to a processor or third party. Hence, we generate for each storage and flow information requirement a data subject intervention requirement with type *review*, effect *access*, and time *anyTime*.

The right to rectification (Article 16) allows data subjects to challenge the accuracy and completeness of their personal data stored by the software or sent to processors or third parties at any time. Hence, we instantiate two additional data subject intervention requirements for each storage and flow information requirement. First, we generate one with type *challengeAccuracy*, effect *correction*, and time *anyTime*, and second, one with type *challengeCompleteness*, effect *amendment*, and time *anyTime*.

The rights to restriction of processing (Article 18) and to object (Article 21) describe that, at any time, data subjects can object to the processing of their personal data and the processing of this personal data shall then be restricted accordingly. Additionally, Article 17 states that in the case of objection to the processing of personal data, the respective personal data shall be erased if there are no overriding legitimate grounds for the processing. Hence, we generate two data subject intervention requirements for each processing information requirement; both with type *object* and time *anyTime* and one with effect *restrictedProcessing* and the other with effect *erasure*.

The right to data portability (Article 20) allows data subjects to request *"the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format [..]"* [10]. Hence, we generate a data subject intervention requirement with type *requestDataCopy*, effect *dataCopy* and time *anyTime* for each collection information requirement. Note that the right to data portability only references the personal data provided by the data subject and not data that results from further processing of the provided data. Because of this, we only generate the intervention requirements for collection information requirements.

In Table 6, we summarize for which processing information requirements which types of data subject intervention requirements are generated.

Table 6. Overview of the generated data subject intervention requirements for processing information requirements.

Processing Information Requirement	Requirements with Intervention Type
Collection, Storage, and Flow	doNotConsent, withdrawConsent, and object
Storage and Flow	review, challengeAccuracy, challenge Completeness
Collection	requestDataCopy

Application to EHS Example

In the EHS example, among others, we get a collection information requirement (CIR) for the patient's personal data *vitalSigns* from the automatic generation described in [8]. Figure 4 shows the collection information requirement and the five data subject intervention requirements (DIR) that are generated for it. As described above, we added to the collection information requirement *consent* as a ground for the processing and the five data subject intervention requirements with the types *requestDataCopy*, *doNotConsent*, *withdrawConsent*, and *object* and the corresponding effects and times. Analogously, data subject intervention requirements are generated for all other processing information requirements. For storage and flow information requirements, the intervention requirement with type *requestDataCopy* is replaced by a requirement with type *review*, and additionally, we have intervention requirements with types *challengeAccuracy* and *challengeCompleteness* (cf. Table 6).

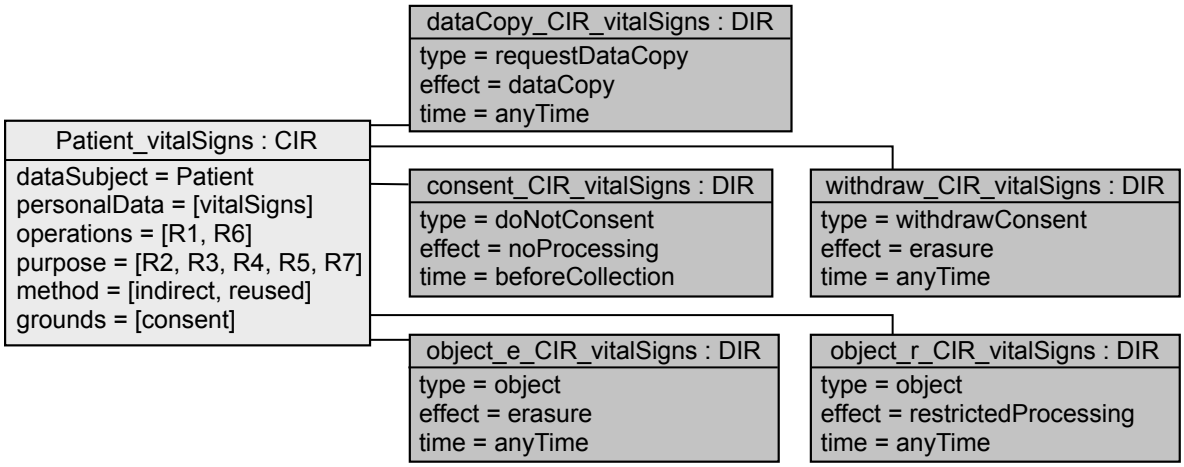

Figure 4. Generated intervention requirements for the collection information requirement for a patient's vital signs.

5.2.2. Exceptional Information Requirement and Authority Intervention Requirement

An exceptional information requirement has the following meaning:

> In the case of a <*case*> concerning the personal data <*personalData*> the <*dataSubject*> and <*authorities*> have to be informed about the occurrence of this event. <*authorities*> have then the power to exercise <*controlOptions*>.

An authority intervention requirement has the following meaning:

> The <*exception.authorities*> shall be able to *type* in the cases described in <*exception*>. The intervention shall result in <*effect*>.

In [8], we do not consider the generation of exceptional information requirements, because we did not consider a legal framework for the generation of the privacy requirements. In this paper, we consider the generation based on the EU General Data Protection Regulation and this regulation implies the need for exceptional information requirements and related authority intervention requirements.

Article 33 is about the notification of a personal data breach to the supervisory authority and Article 34 prescribes the communication of a personal data breach to the data subject. Hence, we generate an exceptional information requirement for each data subject with all personal data of him or her that is processed by the system-to-be with case *dataBreach*. The EU General Data Protection Regulation does not mention intervention options of authorities that are directly related to the occurrence of data breaches. Hence, we do not create related authority intervention requirements.

Article 58 describes the powers of supervisory authorities. These powers imply the need for two additional exceptional information requirements for each data subject and all of his or her personal data. The first exceptional information requirement has the type *authorityRequest* and expresses that the controller has to provide all information to the authorities that these need in order to perform their duties. Associated to this information requirement, we generate an authority intervention requirement with type *obtainAccess*, which represents that authorities can request access to the processed personal data. The second exceptional information requirement has the type *nonCompliance* and represents that authorities have to be informed if personal data is processed in breach with the EU General Data Protection Regulation and describes the actions that supervisory authorities have if this happens. Article 58 implies that this exceptional information requirement shall have an authority intervention requirement of each authority intervention type (except *obtainAccess*) and possible intervention effect (see Table 3). Hence, we generate authority intervention requirements for all of the valid combinations of types (except *obtainAccess*) and effects shown in Table 3.

Application to EHS Example

In the EHS example, we generate three exceptional information requirements (EIR) for the data subject patient and all of his/her personal data: one with the case *dataBreach*, one with *nonCompliance*, and one with *authorityRequest*. The exceptional information requirement with case *authorityRequest* has an authority intervention requirements (AIR) with type *obtainAccess* and the exceptional information requirement with case *nonCompliance* has six authority intervention requirements associated as described above. The exceptional information requirements for patients and the related authority intervention requirements are shown in Figure 5.

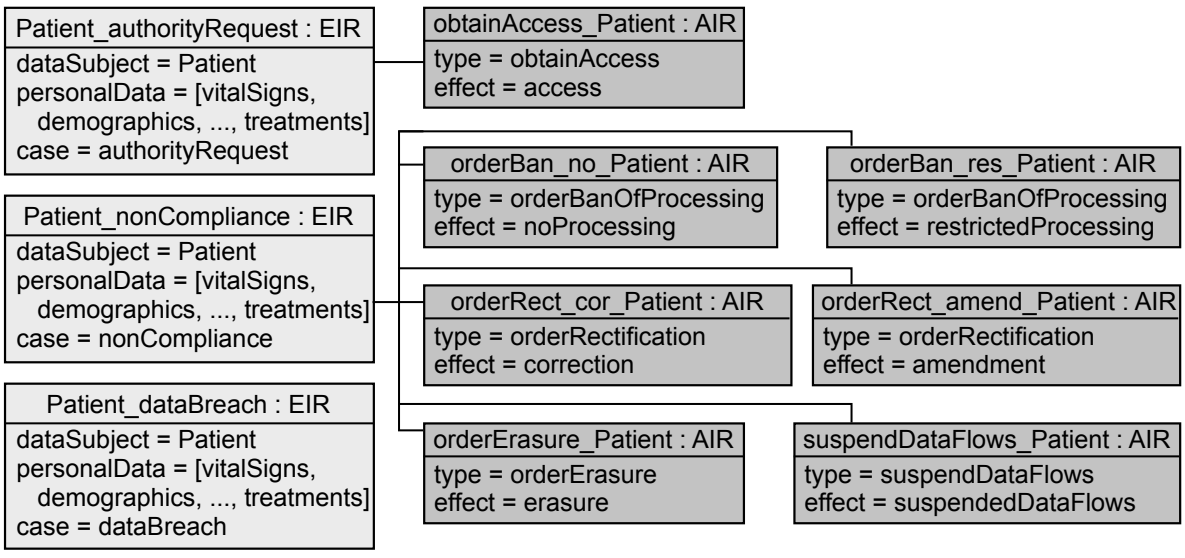

Figure 5. Generated exceptional information requirements and related authority intervention requirements for patients.

5.2.3. Intervention Information Requirement

An intervention information requirement has the following meaning:

The <*data subject*> shall be informed about the progress of his/her interventions based on <*intervention*>.

Article 12 describes that controllers have to inform data subjects about the status of the interventions they requested. Hence, we generate one intervention information requirement for each data subject intervention requirement, as already prescribed by the multiplicities in our proposed taxonomy (see Figure 2).

Application to EHS Example

For each data subject intervention requirement, one intervention information requirement is generated and related to it. For the sake of simplicity, we do not add the seven generated intervention information requirements to Figure 4.

5.3. Adjust Intervenability Requirements

The automatically generated requirements have to be adjusted manually by the user, because not all attributes of the requirements can be set automatically and it is possible that some of the generated requirements are too strong. In the following, we describe the user's possibilities to adjust the generated requirements in conformance with the EU General Data Protection Regulation.

5.3.1. Data Subject Intervention Requirement

The EU General Data Protection Regulations allows some adjustments of the generated intervention requirements for data subjects.

Article 6 states that the processing of personal data shall be based on the data subject's consent, but it provides a list of circumstances under which it is possible to process personal data without the explicit consent of the data subject. These are that the processing is necessary (1) *"for the performance of a contract to which the data subject is a party"* (ProcessingGround *contract* in Figure 2); (2) *"for compliance with a legal obligation"* (ProcessingGround *regulation*); (3) *"to protect the vital interest of the data subject"* (ProcessingGround *vitalInterest*); (4) *"for the performance of a task carried out in the public interest"* (ProcessingGround *publicInterest*); (5) *"for the purposes of the legitimate interests pursued by the controller or by a third party"* (ProcessingGround *controllerInterest*); and (6) *"for the establishment, exercise or defense of legal claims"* (ProcessingGround *legalClaims*). Hence, the user can decide to remove the ProcessingGround *consent* from a processing information requirement if he/she adds at least one of the other grounds. Then the user has also to remove the related data subject intervention requirements with the types *doNotConsent* and *withdrawConsent*. Additionally, we can change the effect of withdrawing consent to *noProcessing* or *restrictedProcessing* according to Article 17 if the processing is also based on other grounds including *contract*, *regulation*, *vitalInterest*, *publicInterest*, *controllerInterest*, or *legalClaims*.

Article 11 states that if the controller processes personal data that does not allow to identify the related data subject, then the controller is not obliged to provide the data subject the rights to access, rectification, erasure, restriction of processing, and data portability, unless the data subject provides additional information that allow his/her identification. Hence, the user can decide to remove data subject intervention requirements of type *review*, *challengeAccuracy*, *challengeCompleteness*, *object*, and *requestDataCopy* if the personal data of the related processing information requirement cannot be related to the individual data subject it belongs to using the information provided by the system-to-be. The processing of aggregated data, instead of data that is linkable to the individual, is an example of a situation in which the controller can decide to remove data subject intervention requirements of the above mentioned types.

Article 17 allows the user to remove data subject intervention requirements with type *object* and effect *erasure* if the processing grounds of the related processing information requirement include *regulation*, *publicInterest*, or *legalClaims*.

For all data subject intervention requirements, the user has to specify the consequences that a data subject has to expect when he/she exercises his/her rights represented by the respective intervention requirement. This is already specified by the multiplicity 1 in Figure 2.

Finally, the user can strengthen the attribute time and decide to make the time at which a data subject can exercise his/her rights stricter in the sense of a linear ordering $<_{AT}$. We define the linear ordering $<_{AT}$ on the enumeration *ActionTime* as follows: *anyTime* $<_{AT}$ *beforeCollection* $<_{AT}$ *beforeUse* $<_{AT}$ *atRecording* $<_{AT}$ *beforeTransmission* $<_{AT}$ *afterRecognition* $<_{AT}$ *onRequest*. The underlying semantics of this linear ordering is that an action time is smaller than another action time if it is stricter in the sense that it applies to more cases than the other (e.g., *anyTime* applies for all points in time) or will take place earlier in time (e.g., *beforeCollection* is earlier than *beforeUse*).

Note that if a data subject intervention requirement is removed, then also its related intervention information requirement is removed from the model, because it has no meaning without the related data subject intervention requirement.

Application to EHS Example

As described in [8], the collection information requirement has to be completed because not all of the information that is documented in a processing information requirement can automatically be derived from the ProPAn model. Hence, we have to specify the controller of the EHS and set it to the *EHSOwner*.

In the EHS example, we do not need to consider consent as a ground for the processing, because the vital signs of patients are collected for purposes in their vital interest. Hence, we can remove the data subject intervention requirements with type *doNotConsent* and *withdrawConsent* that are shown in Figure 4 and we add *vitalInterest* to the grounds of the collection information requirement (see Figure 6). Additionally, the collected vital signs could be important in the case of legal claims and hence, we can also remove the intervention requirement with type *object* and effect *erasure* and we add *legalClaims* to the grounds of the collection information requirement.

In the EHS system, the vital signs are linkable to the individual they belong to and hence, we cannot remove the remaining intervention requirement with type *object* based on Article 11.

Anyway, we have to define the consequences that the intervention will have for data subjects (cf. Figure 2). The resulting data subject requirements together with their related collection information requirement for patients' vital signs are shown in Figure 6.

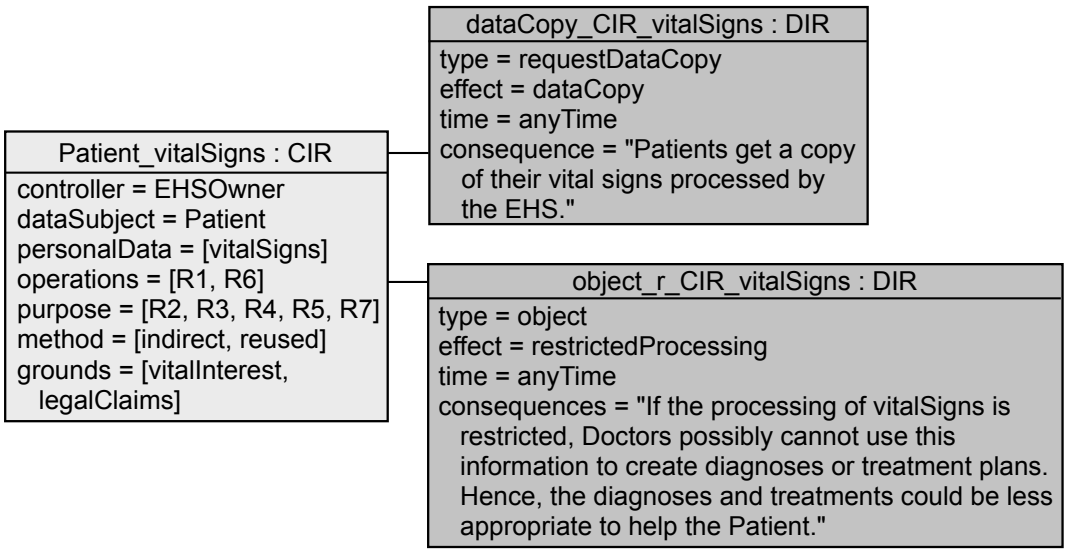

Figure 6. Adjusted intervention requirements for the collection information requirement for a patient's vital signs.

5.3.2. Exceptional Information Requirement

The user has to manually complete the generated exceptional information requirements. The attributes that have to be set for each exceptional information requirement are the controller of the system-to-be and the authorities that the controller has to inform. The European Commission provides a list of the data protection authorities of its member states [54]. This list can be used to determine relevant data protection authorities for the system-to-be.

There are no further possibilities to adjust the generated exceptional information requirements, because informing supervisory authorities about the processing of personal data and data breaches is mandatory if the processing shall comply with the EU Data Protection Regulation.

Application to EHS Example

We instantiate the controller with the *EHSOwner*, as we also did for the collection information requirement shown in Figure 6. Furthermore, as relevant authorities, we added the *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI)* (the German data protection authority) and the *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)* (the data protection authority of the state North Rhine-Westphalia), because we assume that the EHS shall be operated and used in North Rhine-Westphalia. The adjusted exceptional information requirements are shown in Figure 7.

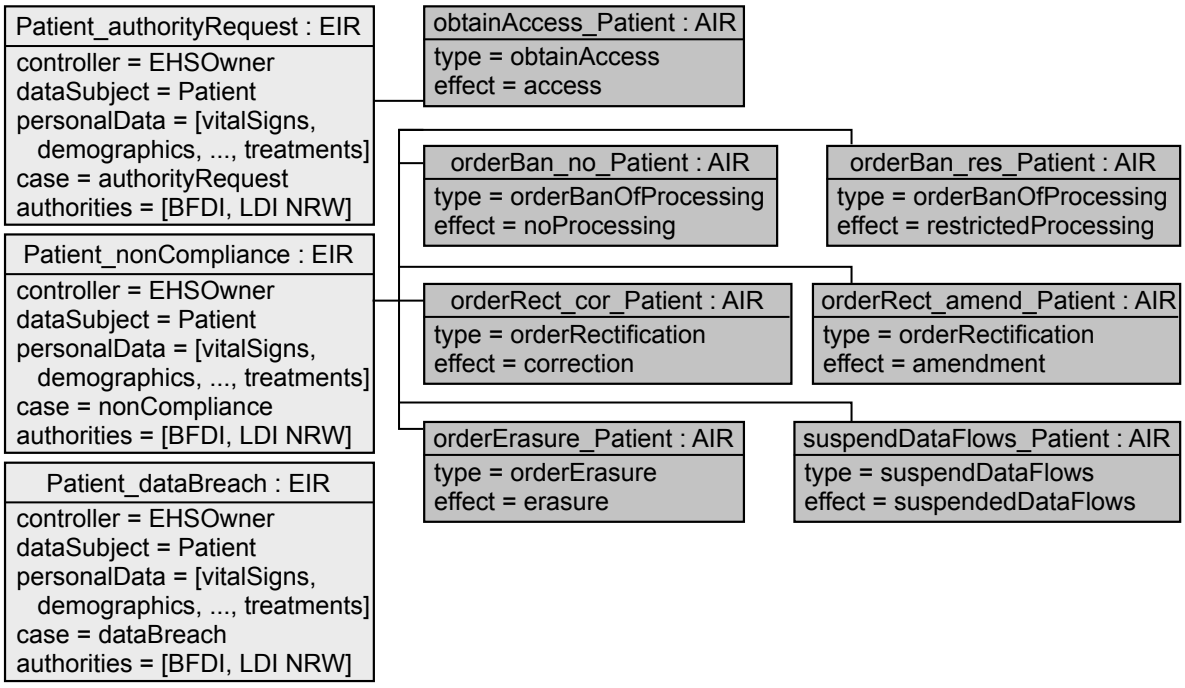

Figure 7. Adjusted exceptional information requirements and related authority intervention requirements for patients.

5.3.3. Authority Intervention Requirement

The EU Data Protection Regulation provides no information about circumstances when the authority intervention requirements do not need to be considered. Hence, a user should only modify the generated requirements after consultation of a legal expert in the field of data protection.

Application to EHS Example

The generated authority intervention requirements are not changed (see Figure 7), because we expect that the data protection authorities could make use of all their powers.

5.3.4. Intervention Information Requirement

The user has to set the controller of the system-to-be for each intervention information requirement. There are no further possibilities to adjust the generated intervention information requirements.

Application to EHS Example

The controller of the intervention information requirements is also set to *EHSOwner*. For the sake of simplicity, we do not show the remaining two intervention information requirements for the data subject information requirements shown in Figure 6.

5.4. Validate Intervenability Requirements

To check whether the user's modifications on the generated intervenability and transparency requirements still comply to the EU General Data Protection Regulation, we developed several validation conditions that allow an automatic validation of the consistency of the adjusted intervenability and transparency requirements. In [8], we already defined several validation conditions for privacy requirements including transparency requirements. In this paper, we extend this list.

5.4.1. Transparency Requirements

In [8], we already proposed seven validation conditions for transparency requirements. In this paper, we enhanced the taxonomy and added intervention requirements to it. Hence, we obtain further validation conditions that check the consistency of transparency requirements and their relations to the intervention requirements. Furthermore, we set up the validation conditions with the aim of complying to the EU General Data Protection regulation in mind. This is, we check whether only the adjustments described in the previous section are performed.

Note that, in [8], we introduced validation conditions for transparency requirements that raise an error if an attribute is not set and warn the user if an attribute with a multiplicity greater than 1 (except counterstakeholder) is empty. These two validation conditions also apply to the newly introduced attributes and intervention information requirements.

From Article 6, we derive that the grounds of a processing information requirement shall contain *consent*, unless the grounds include *contract*, *regulation*, *vitalInterest*, *publicInterest*, *controllerInterest*, or *legalClaims*. Hence, we obtain the following validation condition.

VT8 Raise an error for every processing information requirement whose *grounds* include neither *contract*, *regulation*, *vitalInterest*, *publicInterest*, *controllerInterest*, nor *legalClaims* if its *grounds* do not include *consent*.

Article 6 and 7 imply that if processing is based on consent, then the data subject shall have the options to not consent and to withdraw previously given consent. If the options to not consent and to withdraw previously given consent are presented to a data subject, then this processing is based on consent and should have *consent* as a processing ground. This leads to the following two validation conditions.

VT9 Raise an error for each processing information requirement whose *grounds* include *consent* if no data subject intervention requirements with *type doNotConsent* and *withdrawConsent* are *controlOptions* of the processing information requirement.

VT10 Raise an error for each processing information requirement that has as *controlOptions* data subject intervention requirements with *type doNotConsent* and *withdrawConsent* if its *grounds* do not include *consent*.

As discussed in the previous section, Article 11 states that controllers are not forced to provide intervention options to data subjects if the controller is not able to identify the data subject from the personal data that is processed. Hence, the following validation VT11 to VT15 conditions include as a

precondition that the controller is able to identify the data subject to which the concerned personal data belong.

Due to Article 15, data subjects shall be able to access all their personal data that is stored and provided to others. Hence, we obtain the following validation condition.

VT11 Raise an error for each storage and flow information requirement about *personalData* that the *controller* can uniquely link to the *dataSubject* if it does not have a data subject intervention requirement with *type access* as *controlOption*.

From Article 16, we can derive the right of data subjects to challenge the accuracy and completeness of their stored personal data and personal data provided to others. This leads to the following validation condition.

VT12 Raise an error for each storage and flow information requirement about *personalData* that the *controller* can uniquely link to the *dataSubject* if it does not have a data subject intervention requirement with *type challengeAccuracy* and *challengeCompleteness* as *controlOption*.

The right to erasure (Article 17) says that the effect of objection to the processing shall be the erasure of this data, unless the processing of the concerned personal data is necessary for other legitimate purposes, e.g., compliance with legal obligations. Hence, we get the following validation condition:

VT13 Raise an error for each processing information requirement about *personalData* that the *controller* can uniquely link to the *dataSubject* and whose *grounds* include neither *regulation*, *publicInterest*, nor *legalClaims* if it does not have a data subject intervention requirement with *type object* and *effect erasure* as *controlOption*.

Article 18 describes the right to restrict the processing of personal data. Hence, we obtain the following validation condition:

VT14 Raise an error for each processing information requirement about *personalData* that the *controller* can uniquely link to the *dataSubject* if it does not have a data subject intervention requirement with *type object* and *effect noProcessing* or *restrictedProcessing* as *controlOption*.

The existence of an intervention option related to the right to data portability (Article 20) is checked by the following validation condition.

VT15 Raise an error for each collection information requirement about *personalData* that the *controller* can uniquely link to the *dataSubject* and whose grounds do not include *publicInterest* if it does not have a data subject intervention requirement with *type requestDataCopy* as *controlOption*.

Article 33 is concerned with the occurrence of data breaches and the duties of controllers in the case of such. From this Article, we derived the following validation condition.

VT16 Raise an error for each personal data of a data subject if no exceptional information requirement with *case dataBreach* exists for this data subject and includes the personal data.

From Article 58, we have deduced in Section 5.2.2 the intervention options of supervisory authorities. The following validation conditions check whether theses intervention options are reflected in the model.

VT17 Raise an error for each personal data of a data subject if no exceptional information requirement with *case authorityRequest* exists for this data subject and includes the personal data.

VT18 Raise an error for each exceptional information requirement with *case authorityRequest* if its *controlOptions* do not include an authority intervention requirement with type *obtainAccess*.

VT19 Raise an error for each personal data of a data subject if no exceptional information requirement with *case nonCompliance* exists for this data subject and includes the personal data.

VT20 Raise an error for each exceptional information requirement with *case nonCompliance* if its *controlOptions* do not include authority intervention requirements with type *suspendDataFlows*, *orderBanOfProcessing*, *orderErasure*, and *orderRectification*.

As it is mandatory that supervisory authorities are informed about data breaches and the user has to expect that they will exercise their powers, the user has to instantiate the attribute *authorities* of the exceptional information requirements with the relevant supervisory authorities. Hence, we have the following validation condition.

VT21 Raise an error for each exceptional information requirement if the attribute *authorities* is empty.

Application to the EHS Example

The adjusted intervention requirements for the collection information requirement for a patient's vital signs shown in Figure 6 satisfy all validation conditions that are applicable to it. Table 7 provides on overview of the application of the validation conditions and the reasons for satisfaction and non-applicability.

Table 7. Validation of the collection information requirement for a patient's vital signs and its data subject intervention requirements.

Condition	Result	Reason
VT8	not applicable	*grounds* include *vitalInterest* and *legalClaims*
VT9	not applicable	*grounds* do not include *consent*
VT10	not applicable	no *controlOptions* with type *doNotConsent* and *withdrawConsent* are assigned
VT11	not applicable	requirement is neither a storage nor flow information requirement
VT12	not applicable	requirement is neither a storage nor flow information requirement
VT13	not applicable	*grounds* includes *legalClaims*
VT14	satisfied	a *controlOption* with type *object* and effect *restrictedProcessing* exists
VT15	satisfied	a *controlOption* with type *requestDataCopy* exists
VT16	not applicable	requirement is not an exceptional information requirement
VT17	not applicable	requirement is not an exceptional information requirement
VT18	not applicable	requirement is not an exceptional information requirement
VT19	not applicable	requirement is not an exceptional information requirement
VT20	not applicable	requirement is not an exceptional information requirement
VT21	not applicable	requirement is not an exceptional information requirement

The exceptional information requirements shown in Figure 7 also satisfy all validation conditions that are applicable to them, but for the sake of simplicity we omit a detailed explanation.

5.4.2. Intervenability Requirements

To check whether the user correctly adjusted the generated intervenability requirements, we also provide validation conditions that can automatically be checked by the ProPAn tool.

First, we introduce a validation condition that checks whether the attributes and links of intervention requirements are instantiated.

VI1 Raise an error for each data subject intervention requirement where an attribute is not set.

In Tables 3 and 4, we presented the valid combinations of intervention types and intervention effects for authority and data subject intervention requirements. The following validation condition checks whether all intervention requirements comply to these tables.

VI2 Raise an error for each intervention requirement if the combination of *type* and *effect* does not comply to the mappings provided in Tables 3 and 4.

From Articles 6, 7, and 9, we can derive constraints on the time when data subjects shall be able to exercise their intervention options. From these Articles, we derive the following validation conditions.

VI3 Raise an error for each data subject intervention requirement that is a *controlOption* of a collection information requirement, if its *time* is not $\leq_{AT}$ *beforeProcessing*.

VI4 Raise an error for each data subject intervention requirement that is a *controlOption* of a flow information requirement, if its *time* is not $\leq_{AT}$ *beforeTransmission*.

VI5 Raise an error for each data subject intervention requirement that is a *controlOption* of a storage information requirement, if its *time* is not $\leq_{AT}$ *atRecording*.

The right of access by the data subject (Article 15) implies following the validation condition that prescribes to which processing information requirements a data subject intervention requirement with type *access* may be associated and that its time has to be *anyTime*.

VI6 Raise an error for each data subject intervention requirement with *type access* if it is not a *controlOption* of a storage or flow information requirement.

VI7 Raise an error for each data subject intervention requirement with *type access* if its *time* is not *anyTime*.

From Article 16, we can derive that data subjects can challenge the accuracy and completeness of their stored personal data and personal data provided to others at any time. Hence, we obtain the following two validation conditions.

VI8 Raise an error for each data subject intervention requirement with *type challengeAccuracy* or *challengeCompleteness* if it is not a *controlOption* of a storage or flow information requirement.

VI9 Raise an error for each data subject intervention requirement with *type challengeAccuracy* or *challengeCompleteness* if its *time* is not *anyTime*.

From Articles 7, 18, 20, and 21, we can derive a further validation condition concerning the time when data subjects shall be able to exercise their intervention options.

VI10 Raise an error for each data subject intervention requirement with *type withdrawConsent*, *object*, or *requestDataCopy* if its *time* is not *anyTime*.

The right to erasure, also known as the right to be forgotten (Article 17), says that the effect of withdrawing consent to the processing shall be the erasure of this data, unless the processing of the concerned personal data is necessary for other legitimate purposes, e.g., compliance with legal obligations. Hence, we get the following validation condition:

VI11 Raise an error for each data subject intervention requirement with *type withdrawConsent* that is a *controlOption* of a processing information requirement whose *grounds* include neither *contract*, *regulation*, *vitalInterest*, *publicInterest*, *controllerInterest*, nor *legalClaims* if this data subject intervention requirement does not have the *effect erasure*.

Application to the EHS Example

All instances of data subject and authority intervention requirements shown in Figures 6 and 7 satisfy the defined validation conditions. For the sake of simplicity, we show and reason which validation conditions are satisfied by and applicable to the data subject intervention requirement *object_r_CIR_vitalSigns* in Table 8.

Table 8. Validation of the data subject intervention requirement of the type of object shown in Figure 6.

Condition	Result	Reason
VI1	satisfied	all attributes are set (the intervention information requirement is not shown)
VI2	satisfied	the combination of *object* and *restrictedProcessing* exists in Table 4
VI3	satisfied	$anyTime \leq_{AT} beforeProcessing$
VI4	not applicable	requirement is not related to a flow information requirement
VI5	not applicable	requirement is not related to a storage information requirement
VI6	not applicable	requirement does not have type *access*
VI7	not applicable	requirement does not have type *access*
VI8	not applicable	requirement does not have type *challengeAccuracy* or *challengeCompleteness*
VI9	not applicable	requirement does not have type *challengeAccuracy* or *challengeCompleteness*
VI10	satisfied	time is *anyTime*
VI11	not applicable	requirement does not have type *withdrawConsent*

6. Conclusions

The contributions of this paper can be divided into two parts. The first part consists of the contributions that we already presented in [6], with the difference that we used the EU General Data Protection Regulation in this paper instead of the Draft of the EU General Data Protection Regulation that was used in [6] to derive intervenability requirements from it. The second part consists of the novel contributions of this paper that extend [6].

In the first part, (1) we systematically derived requirements for the privacy goal of intervenability and related transparency requirements from the ISO 29100 standard [9] and the EU General Data Protection Regulation [10]. (2) We then integrated these requirements into an existing metamodel for transparency requirements [7]. The new metamodel provides an overview of the identified kinds of transparency and intervenability requirements and how these are related to each other. The metamodel shall furthermore help requirements engineers to identify and document the transparency and intervenability requirements relevant to them and the information needed to address the transparency and intervenability requirements. (3) We performed a systematic literature review and provide an overview of the relevant research related to intervenability requirements. (4) We validated that our taxonomy contains all necessary aspects mentioned in the identified literature. The literature review showed that all aspects of the privacy goal of intervenability mentioned in the literature are reflected in the proposed taxonomy. Furthermore, we did not find any literature that presents intervenability requirements and their relation to transparency requirements in such a structured, detailed, and complete manner.

In the second part, we showed how intervenability requirements can (1) automatically be generated based on artifacts provided by the ProPAn method and rules derived from the EU General Data Protection Regulation; (2) we provide guidance how these generated requirements have to be completed and how they can be adjusted under the consideration of the EU Data Protection Regulation; and (3) we provide validation conditions that can be used to automatically check whether the users adjustments still comply to the needs implied by the EU General Data Protection Regulation. All steps of our method are integrated into the ProPAn tool that is able to execute the generation and validation fully automatically.

We believe that our taxonomy is flexible enough to also represent intervenability and transparency requirements from other regulations and standards, because our proposed metamodel of the taxonomy can easily be adopted and extended. In these cases, our metamodel can be enhanced with, e.g., further intervention types and effects. These can easily be added to the corresponding enumerations (cf. Figure 2). Additionally, our method for the generation, adjustment, and validation of intervenability requirements could be adopted to comply to other regulations or standards. Note that such an adoption is a non-trivial task that relies on the knowledge of legal experts. This is because different regulations may lead to contradicting requirements, and we need the help of legal experts to derive rules that lead

to a consistent set of requirements that are as compliant as possible to the regulations that have to be considered.

For future research, we identified two open research questions. (1) Which kinds of threats to transparency and intervenability requirements exist? (2) Which technologies exist that implement transparency and intervenability requirements or mitigate threats to transparency and intervenability requirements? To address the latter two questions, we plan to set up a catalog of threats that possibly lead to a violation of the identified transparency and intervenability requirements and related mechanisms that may be used to mitigate the identified threats. Based on this catalog, we want to develop a systematic method to identify the relevant threats for a given set of functional requirements and appropriate countermeasures in order to perform a privacy risk assessment.

Acknowledgments: We thank Sylbie Sabit who provided a starting point for this research with her master thesis [55]. This work was partially supported by the Deutsche Forschungsgemeinschaft (DFG) under grant No. GRK 2167, Research Training Group "User-Centred Social Media".

Author Contributions: Rene Meis wrote the paper and Maritta Heisel provided substantial feedback that improved the paper. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIR	AuthorityInterventionRequirement
DIR	DataSubjectInterventionRequirement
EHR	Electronic Health Record
EHS	Electronic Health System
EIR	ExceptionalInformationRequirement
IIR	InterventionInformationRequirement
IR	IntervenabilityRequirement
OECD	Organisation for Economic Co-operation and Development
PET	Privacy Enhancing Technology
PIR	ProcessingInformationRequirement
ProPAn	Problem-based Privacy Analysis
RIT	Relation between intervenability and transparency requirements
SDFG	Stakeholder Data Flow Graph
UML	Unified Modeling Language

References

1. GSMA. MOBILE PRIVACY: Consumer Research Insights and Considerations For Policymakers. Available online: http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf (accessed on 20 June 2016).
2. Symantec. State of Privacy Report 2015. Available online: https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf (accessed on 20 June 2016).
3. Quah, A.M.Y.; Röhm, U. User Awareness and Policy Compliance of Data Privacy in Cloud Computing. In Proceedings of the First Australasian Web Conference–Volume 144, Adelaide, Australia, 29 January–3 February 2013; pp. 3–12.
4. Ackerman, M.S.; Cranor, L.F.; Reagle, J. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. In Proceedings of the 1st ACM Conference on Electronic Commerce (EC '99); Denver, CO, USA, 3–5 November 1999; pp. 1–8.
5. Hansen, M. Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In *Privacy and Identity Management for Life*; Camenisch, J., Crispo, B., Fischer-Hübner, S., Leenes, R., Russello, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 14–31.
6. Meis, R.; Heisel, M. Understanding the Privacy Goal Intervenability. In *Trust, Privacy, and Security in Digital Business*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 79–94.

7. Meis, R.; Heisel, M.; Wirtz, R. A Taxonomy of Requirements for the Privacy Goal Transparency. In *Trust, Privacy, and Security in Digital Business*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 195–209.
8. Meis, R.; Heisel, M. Computer-Aided Identification and Validation of Privacy Requirements. *Information* **2016**, *7*, 28.
9. International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). ISO/IEC 29100:2011 Information Technology–Security Techniques–Privacy Framework. Available online: https://www.iso.org/standard/45123.html (accessed on 3 March 2017).
10. European Commission. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (accessed on 14 December 2016).
11. Organisation for Economic Co-operation and Development (OECD). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available online: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed on 5 March 2017).
12. US Federal Trade Commission. Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress. Available online: https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission (accessed on 5 March 2017).
13. Jalali, S.; Wohlin, C. Systematic Literature Studies: Database Searches vs. Backward Snowballing. In Proceedings of the ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, Lund, Sweden, 19–20 September 2012; pp. 29–38.
14. CORE2014. Available online: http://www.core.edu.au/conference-portal (accessed on 20 June 2016).
15. Bier, C. How Usage Control and Provenance Tracking Get Together—A Data Protection Perspective. Presented at 2013 IEEE Security and Privacy Workshops (SPW), San Diego, CA, USA, 23–24 May 2013; pp. 13–17.
16. Hoepman, J.H. In Privacy Design Strategies—(Extended Abstract). In *ICT Systems Security and Privacy Protection*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 446–459.
17. Mouratidis, H.; Islam, S.; Kalloniatis, C.; Gritzalis, S. A framework to support selection of cloud providers based on security and privacy requirements. *J. Syst. Softw.* **2013**, *86*, 2276–2293.
18. Miyazaki, S.; Mead, N.; Zhan, J. Computer-Aided Privacy Requirements Elicitation Technique. Presented at IEEE 2008 Asia-Pacific Services Computing Conference (APSCC '08), Yilan, Taiwan, 9–12 December 2008; pp. 367–372.
19. Kalloniatis, C.; Mouratidis, H.; Vassilis, M.; Islam, S.; Gritzalis, S.; Kavakli, E. Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Comput. Stand. Interfaces* **2014**, *36*, 759–775.
20. Kalloniatis, C. Designing Privacy-Aware Systems in the Cloud. In *Trust, Privacy and Security in Digital Business*; Lecture Notes in Computer Science (LNCS); Springer: Berlin/Heidelberg, Germany, 2015; Volume 9264, pp. 113–123.
21. Spiekermann, S.; Cranor, L. Engineering Privacy. *IEEE Trans. Softw. Eng.* **2009**, *35*, 67–82.
22. Makri, E.; Lambrinoudakis, C. Privacy Principles: Towards a Common Privacy Audit Methodology. In *Trust, Privacy and Security in Digital Business*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9264, pp. 219–234.
23. Acquisti, A.; Adjerid, I.; Brandimarte, L. Gone in 15 Seconds: The Limits of Privacy Transparency and Control. *IEEE Secur. Priv.* **2013**, *11*, 72–74.
24. Masiello, B. Deconstructing the Privacy Experience. *IEEE Secur. Priv.* **2009**, *7*, 68–70.
25. Krol, K.; Preibusch, S. Effortless Privacy Negotiations. *IEEE Secur. Priv.* **2015**, *13*, 88–91.
26. Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* **2011**, *1*, 3–32
27. Komanduri, S.; Shay, R.; G. Norcie, B.U.; Cranor, L.F. AdChoices? Compliance with Online Behavioral Advertising Notice and Choice Requirements. Available online: http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Komanduir.Final_.pdf (accessed on 20 June 2016).

28. Cranor, L.F. Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *J. Telecomm. High Tech. L.* **2012**, *10*, 273–308.
29. Wicker, S.; Schrader, D. Privacy-Aware Design Principles for Information Networks. *Proc. IEEE* **2011**, *99*, 330–350.
30. Strickland, L.S.; Hunt, L.E. Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions. *J. Assoc. Inf. Sci. Technol.* **2005**, *56*, 221–234.
31. Sheth, S.; Kaiser, G.; Maalej, W. Us and Them: A Study of Privacy Requirements Across North America, Asia, and Europe. In Proceedings of the 36th International Conference on Software Engineering (ICSE 2014), Hyderabad, India, 31 May–7 June 2014; pp. 859–870.
32. Fhom, H.; Bayarou, K. Towards a Holistic Privacy Engineering Approach for Smart Grid Systems. Presented at 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Changsha, China, 16–18 November 2011; pp. 234–241.
33. Antón, A.I.; Earp, J.B.; Reese, A. Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy. In Proceedings of the IEEE Joint International Conference on Requirements Engineering, Essen, Germany, 9–13 September 2002; pp. 23–31.
34. Antón, A.I.; Earp, J.B. A requirements taxonomy for reducing Web site privacy vulnerabilities. *Requir. Eng.* **2004**, *9*, 169–185.
35. Van Der Sype, Y.S.; Seigneur, J.M. Case study: Legal requirements for the use of social login features for online reputation updates. In Proceedings of the 29th Annual ACM Symposium on Applied Computing (SAC '14), Gyeongju, Korea, 24–28 March 2014; pp. 1698–1705.
36. Basso, T.; Moraes, R.; Jino, M.; Vieira, M. Requirements, design and evaluation of a privacy reference architecture for web applications and services. In Proceedings of the 30th Annual ACM Symposium on Applied Computing (SAC '15), Salamanca, Spain, 13–17 April 2015; pp. 1425–1432.
37. Lobato, L.; Fernandez, E.; Zorzo, S. Patterns to Support the Development of Privacy Policies. Presented at International Conference on Availability, Reliability and Security, 2009 (ARES '09), Fukuoka, Japan, 16–19 March 2009; pp. 744–749.
38. Caron, X.; Bosua, R.; Maynard, S.B.; Ahmad, A. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Comput. Law Secur. Rev.* **2016**, *32*, 4–15.
39. Borgesius, F.Z. Informed Consent: We Can Do Better to Defend Privacy. *IEEE Secur. Priv.* **2015**, *13*, 103–107.
40. Breaux, T. Privacy Requirements in an Age of Increased Sharing. *IEEE Softw.* **2014**, *31*, 24–27.
41. Langheinrich, M. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*; LNCS 2201; Springer: Berlin/Heidelberg, Germany, 2001; pp. 273–291.
42. Feigenbaum, J.; Freedman, M.; Sander, T.; Shostack, A. Privacy Engineering for Digital Rights Management Systems. In *Security and Privacy in Digital Rights Management*; LNCS 2320; Springer: Berlin/Heidelberg, Germany, 2002; pp. 76–105.
43. Wright, D.; Raab, C. Privacy principles, risks and harms. *Int. Rev. Law Comput. Technol.* **2014**, *28*, 277–298.
44. Guarda, P.; Zannone, N. Towards the Development of Privacy-aware Systems. *Inf. Softw. Technol.* **2009**, *51*, 337–350.
45. Hedbom, H. A Survey on Transparency Tools for Enhancing Privacy. In *The Future of Identity in the Information Society*; IFIP AICT 298; Springer: Berlin/Heidelberg, Germany, 2009; pp. 67–82.
46. Smith, H.J.; Dinev, T.; Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Q.* **2011**, *35*, 989–1016.
47. ProPAn Tool. Available online: http://www.uml4pf.org/ext-propan/ (accessed on 7 March 2017).
48. Jackson, M. *Problem Frames: Analyzing and Structuring Software Development Problems*; Addison-Wesley: Boston, MA, USA, 2001.
49. Meis, R. Problem-Based Consideration of Privacy-Relevant Domain Knowledge. In *Privacy and Identity Management for Emerging Services and Technologies*; IFIP AICT 421; Springer: Berlin/Heidelberg, Germany, 2014; pp 150–164.
50. Beckers, K.; Faßbender, S.; Gritzalis, S.; Heisel, M.; Kalloniatis, C.; Meis, R. Privacy-Aware Cloud Deployment Scenario Selection. In *Trust, Privacy, and Security in Digital Business*; LNCS 8647; Springer: Berlin/Heidelberg, Germany, 2014; pp. 94–105.

51. Beckers, K.; Faßbender, S.; Heisel, M.; Meis, R. A Problem-based Approach for Computer Aided Privacy Threat Identification. In *Privacy Technologies and Policy*; LNCS 8319; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–16.
52. Meis, R.; Heisel, M. Supporting Privacy Impact Assessments using Problem-based Privacy Analysis. *Softw. Technol.* **2016**, *586*, pp. 79–98.
53. Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS). Available online: http://www.nessos-project.eu/ (accessed on 7 March 2017).
54. European Data Protection Authorities. Available online: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm (accessed on 14 December 2016).
55. Sabit, S. Consideration of Intervenability Requirements in Software Development. Master Thesis, University of Duisburg-Essen, Duisburg, Germany, 2015.