Proceedings of the Federated Conference on Computer Science and Information Systems pp. 555–563
DOI: 10.15439/2019F275
ISSN 2300-5963 ACSIS, Vol. 18

Deriving Workflow Privacy Patterns from Legal Documents

Marcin Robak
Hochschule für Telekommunikation Leipzig, Germany
Email: robak@hft-leipzig.de

Erik Buchmann
Hochschule für Telekommunikation Leipzig, Germany
Email: buchmann@hft-leipzig.de

***Abstract*—The General Data Protection Regulation (GDPR) has strengthened the importance of data privacy and protection for enterprises offering their services in the EU. An important part of intensified efforts towards better privacy protection is enterprise workflow (re)design. In particular, the GDPR as strengthen the imperative to apply the *privacy by design* principle when (re)designing workflows. A conforming and promising approach is to model privacy relevant workflow fragments as Workflow Privacy Patterns (WPPs). Such WPPs allow to specify abstract templates for recurring data-privacy problems in workflows. Thus, WPPs are intended to support workflow engineers, auditors and privacy officers by providing pre-validated patterns that comply with existing data privacy regulations. However, it is unclear yet how to obtain WPPs systematically with an appropriate level of detail.**

In this paper, we introduce our approach to derive WPPs from legal texts and similar normative regulations. We propose a structure of a WPP, which we derive from pattern approaches from other research areas. We also introduce a framework that allows to design WPPs which make legal regulations accessible for persons who do not possess in-depth legal expertise. We have applied our approach to different articles of the GDPR, and we have obtained evidence that we can transfer legal text into a structured WPP representation. If a workflow correctly implements a WPP that has been designed that way, the workflow automatically complies to the respective fragment of the underlying legal text.

I. Introduction

PRIVACY and data protection are within the scope of interest of enterprises since years. Most current privacy related efforts in enterprises are driven by the General Data Protection Regulation (GDPR) [1] which came into action in May 2018 at the EU level. The regulation describes a set of imperatives enterprises have to consider in their workflows. A workflow is a business process automation, where information and tasks are transferred between participants according to business rules. Regarding GDPR, special attention should be paid to the Article 25 ('data protection by design and by default'). It obliges businesses to implement privacy-aware data management processes in all workflows that handle personal data. This is a complex and challenging task, because all respective workflows must be reconsidered from a privacy perspective. These requirements can originate from privacy norms written in national and international law texts. They also can result from a company's Binding Corporate Rules.

Workflow Privacy Patterns (WPPs) have been introduced by [2]. The idea of WPPs is to compile complex data privacy norms into a compact representation which support workflow creators and analysts with designing and verifying workflows. WPP have to be pre-validated by data privacy experts and must be understandable for a wider audience. Workflow engineers without legal expertise shall be able to assess if the implementation of a particular WPP allows to create a privacy-compliant workflow. The implementation of a WPP shall not require legal expertise. Also, it shall be easier for a workflow analyst to find out if a workflow contains a WPP, than to conduct a privacy assessment unassisted. Thus, the WPP approach is promising. However, what is currently missing is a library of validated WPP designs. This is due to the fact that there is no approach to obtain WPPs from legal sources. In this paper, we introduce our approach to derive WPPs from complex legal texts containing data privacy norms.

Our research method is based on the design science [3] approach. We start with a problem statement, then we systematically compile a set of requirements for 'good' WPPs. Based on the structure of legal documents, we deduce which information must be represented in a WPP, and we provide a framework to extract this information from documents such as binding corporate rules, national and international law texts or compliance rules. We show applicability of our approach with two different use cases.

Our work indicates that it is possible to create WPPs in a structured way, resulting in WPPs with practical potential. This could foster companies in fulfilling privacy obligations which promote customer privacy protection.

Paper structure: The next section describes fundamentals and legal concepts related to our work and serves as a starting point for our research. In Section III we define a structure of a WPP, and in the Section IV we describe how to fill it with content derived from legal documents. This section also shows exemplarily how this framework can be applied to a fragment from the GDPR. Finally, Section V concludes.

II. Related Work

In this section we discuss legal and research foundation related to data privacy. We will also describe the concept of patterns which is in use in the computer science and other industry areas.

A. Privacy concepts

The GDPR describes several requirements on privacy; most of them are well-proven concepts. The GDPR has an impact

on workflow designs on three different levels of abstraction:

On a global level, the GDPR obligates the enterprises to take care about data protection already *while planning and designing* their workflows. Specifically, Article 25 requires that the processing of personal data shall be planned and executed always in a way which supports privacy. This requirement is known also as privacy (or data protection) by design and by default [4]. It results from postulate of instant protection, and from the observation that effective data protection should not be realized only by reactive or retrospective actions [5]. To obtain privacy by design, other two levels must be taken care of. We describe them below.

The second level of the GDPR's impact on workflows is the *requirement for particular actions* in specific situations. Several Articles describe situations for which particular actions must be taken. For example, Article 15 ('right of access') calls for businesses that provide information about the amount of personal data, the purposes of the processing, its storage period, etc., as soon as a person files a request for information. Other articles describe further situations the enterprises must be prepared for. It can be changing or erasing personal data, if a person asks for it in line with the Article 16 ('right for rectification') or Article 17 ('right to be forgotten').

The third level is constituted by the *principles* relating to the processing of personal data. They do not describe specific actions or workflow fragments, but they still affect workflows. Some of these principles are described in the Article 5. For example 'purpose limitation' principle requires that the data collected to fulfill one particular business task should not be used for other purposes. The data minimization principle specifies that the amount of personal data which is collected or handled should be limited to the minimum required to finish the business task.

B. Patterns

Design patterns are reusable solutions for recurring problems. Design patterns have been proposed in several fields. Already in 1977 Alexander [6] wrote "Each pattern describes a problem which occurs over and over again in our environment, and then describes the core of the solution of the problem, in such way that you can use this solution a million times over, without ever doing it the same way twice". The same kind of thinking was adapted in the fields of software engineering [7] and IT architecture [8].

In the field of workflow modeling, workflow patterns have been introduced [9]. Different perspectives of workflow models can be considered [10], depending on the intended use of the model. Well-known perspectives are 'control flow', 'data', 'resources', 'functional' and 'operational'. Most workflow patterns [11] focus on the first three perspectives. For example, [12] lists 43 different control-flow patterns ranging from the synchronization of parallel workflows to the explicit termination of workflows. Patterns regarding the data perspective [13] consider the visibility of data, data-driven interactions, the transfer of data and its transfer routes. Patterns such as 'Role-based allocation' [14] address the life cycle of work items from the resources perspective. [15], [16] present exception handling patterns.

In the area of data privacy, collections of software design patterns have been already proposed [17], [18]. Such collections include options to collect, process and share personal data in a legal way, e.g., by using anonymization, onion routing or implied consent. However, a structured collection of design patters for the data-privacy perspective in workflows does not exist so far.

C. Representation of privacy requirements

In general, three approaches exist to integrate privacy requirements into workflows. They vary in the degree of abstraction and the degree of formalization.

Numerous 'best practice' *implementation guides* have been written by privacy authorities, privacy officers and law firms. Such guides contain textual descriptions of steps needed to handle legal obligations. For example, a guide could translate a GDPR Article into an intuitive description of steps which have to be performed. In many cases the guides are tailored to specific industry sectors. However, such guides are less structured than the legal articles. This induces some degree of freedom when implementing them into workflows. Thus, it is difficult to ensure that a workflow designed on basis of a guide is indeed compliant with the regulation.

Checklists allow to perform a target-actual comparison in a structured way. A checklist reduces the effort needed to incorporate legal requirements into workflows. A legal article is distilled to a list of capabilities which must be implemented. However, it is difficult to express some legal obligations only in form of one-dimensional checklists. For example, it would be confusing to represent the right of access as a checklist. This is because the right of access is interwoven with other articles of the GDPR, depending on aspects such as data transfers into third countries or conflicts with the rights of other persons.

Finally, industry-specific *reference models* provide optimized workflow models in a semi-formal language such as EPC [19] that handle typical privacy obligations. For example, a domain expert could define a reference model for handling incoming requests for access in a typical retailer scenario. Thus, the reference model contains best practices in a specific application domain. A workflow engineer could adapt this model to the workflows of his company. However, a reference model does not ensure that its implementation into the workflows of a company is correct regarding the privacy obligation. This has two reasons: Firstly, languages such as EPC or BPMN do not allow to model all obligations mentioned in privacy regulations, e.g., storage periods or data transfers to foreign countries with less developed privacy standards. Secondly, the workflow engineer has a high degree of freedom when adapting the reference model to his company.

III. Deriving Workflow Privacy Patterns

Workflow models automate business processes that execute specific business tasks. To design a workflow model, a workflow engineer analyzes business objectives, company structure,

key performance indicators, etc. But also legal obligations must be met. This is where data privacy requirements come into play. They have an impact on workflow design and are involved in several aspects of workflows. For example, the order of activities (the sequence flow order) in a workflow is vital for privacy. A natural person must give consent *first*, before his data is stored or processed. The data flow within workflows is another important aspect. Authorization and authentication for gaining data access must be carefully planned. Also execution exceptions have the potential to violate data privacy regulations, say, if an activity on personal data cannot be completed without involving third parties.

Consider Text 1, which we will use as a running example in this paper. It shows a typical article from the GDPR.

Text 1 (Fragment of GDPR's Article 15 - Right of access):

> 1. *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*
>   *(a) the purposes of the processing;*
>   *(b) the categories of personal data concerned;*
>   *(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
>   *(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
>   *(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
>   *(f) the right to lodge a complaint with a supervisory authority;*
>   *(...)*
> 2. *Where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.*
> 3. *The controller shall provide a copy of the personal data undergoing processing. (...)*

Staying compliant with such legal regulations implies many consequences for a company's workflows. Enterprises must be prepared for the case when a customer places such access enquiry and they must be able to react accordingly.

A. Problem Statement

A WPP is a translation of one or more privacy obligations into a semi-formal specification, which can be integrated into a workflow model [2]. WPPs support enterprises to be compliant with data privacy regulations. In particular, WPPs shall foster planning, implementing and auditing of workflows handling personal data. In order to find out how such a WPP must be structured and how it can be obtained in a systematic way, we need to consider the capabilities of the WPP users, and we need to define requirements that a WPP must fulfill in order to be applicable.

a) User roles: We have analyzed which different roles are involved in creation and use of WPPs. Our focus was on the functions the roles must fulfill, and which knowledge and which skills are needed in this regard. We have identified three distinct user roles:

WPP creator This role develops a WPP from a particular data privacy norm. This role has legal expertise needed to identify all information from various legal sources, that must be considered in order to implement privacy-compliant workflows. This skill is needed to be able to mirror the legal norm(s) semantically. The WPP creator needs background knowledge on workflow modeling to provide syntactically correct WPPs.

Workflow engineer This role models workflows with the help of WPPs. The workflow engineer implements WPPs into existing workflows or creates new workflows according to a WPP specification. This role needs domain knowledge on the workflow domain and workflow modeling skills, but it doesn't need to possess legal knowledge.

Privacy officer This role verifies and documents if workflows are compliant with data privacy norms. In this role can be a employee or an external auditor. A privacy officer has sufficient domain knowledge and legal expertise to find out, if existing workflow model meets certain privacy obligation.

b) Requirements for WPPs: From the intended use of the WPPs and the expertise of the user roles, we have derived three requirements for WPPs:

R1 WPPs are a variant of design patterns. Thus, WPPs have to meet all *general requirements for design patterns*, e.g. completeness, understandability and reusability.

R2 Because the workflow engineer may lack legal expertise, a WPP must contain *all information necessary* to model or validate a certain privacy obligation. For example, if a WPP is a specification for the implementation of the 'right of access' - as shown in Text 1 -, then it must be possible to create a privacy-compliant workflow on the basis of this WPP only, i.e., without having to consider additional legal texts.

R3 WPPs must be modular to enable *linking of WPPs*. This is particularly important, as privacy obligations often are spread over several articles or multiple legal texts.

Given these requirements, we will now explore options to structure WPPs. We start by deriving an information model to express information from legal norms in a WPP. In the next section, we propose our framework to compile WPPs from legal texts.

Fig. 1. Structure of legal texts

B. Structures of legal texts and design patterns

In this subsection we compare the structures of legal texts and design patterns. Obligations in legal texts typically follow a well-defined structure, as shown in Figure 1. A legal obligation is described by

(1) **the facts of the case** and
(2) **the legal consequences**.

The facts of the case specify

(1a) the *general criteria* for the applicability of the norm and
(1b) the *circumstances* under which a certain legal norm shall bee applied.

The facts of the case result in an if-then form. Thus, the legal norm or corporate rule can be always interpreted as 'if all prerequisites are met, then the consequences apply'. The consequences in turn can be either

(2a) a *course of action* that must be taken or
(2b) a *yes/no-conclusion* in the sense 'if all prerequisites are met, then the regulated action is lawful'.

In a case of our running example, the general criteria for the applicability of the norm (1a) are described in Art. 2, 3 GDPR (Text 2, 3). The norm applies if the company handles personal data related to activities in the EU.

Text 2 (Fragment of Article 2 GDPR): Material Scope

> *1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which(...)*

Text 3 (Fragment of Article 3 GDPR): Territorial Scope

> *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, (...)*

The circumstances (1b) for a person claiming access rights are described in the first paragraph of Art. 15 GDPR (Text 1). It says that the company must actually possess information about this person. The legal consequence (2) is described in the subsequent paragraphs of Art. 15. The consequence requires the company to provide certain information (2a), according to further dependencies.

Design patterns consist of three components, as described in the previous subsection: (i) the *context* the pattern can be applied to, (ii) the *problem* description that allows the engineer to decide, if the pattern is useful for specific design problem, and (iii) a generic *solution* for the described problem [20]. Observe that the general structure of design patterns is similar to the structure of obligations in legal texts; this is shown in the Figure 2. Thus, it seems appropriate to define a WPP alike. To this end, we distinguish **activity patterns** where the consequence is a course of action (2a), and **check pattern** that result in a yes/no-conclusion (2b).

C. Options to represent legal texts

In order to obtain evidence on approaches to structure a WPP, we have conducted a series of preliminary experiments.

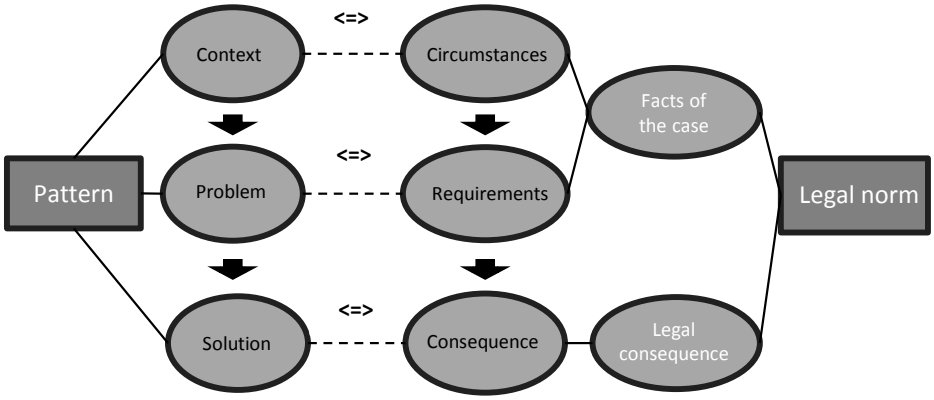

Fig. 2. Relation between legal texts and design patterns

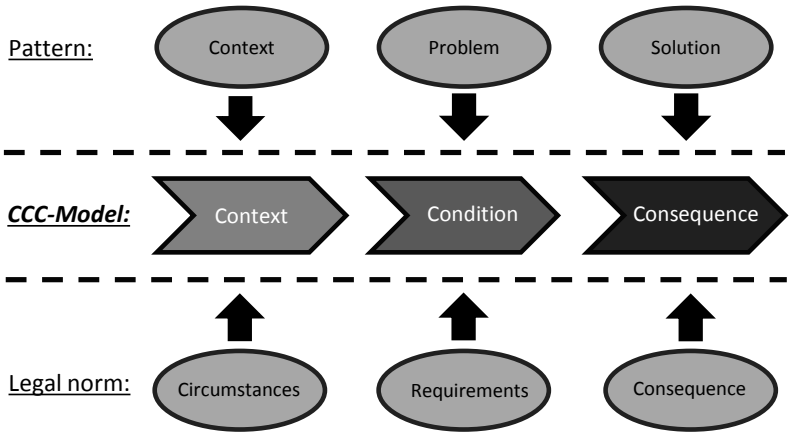

Fig. 3. CCC-Model

In particular, we have asked a class of master's students to model the facts of the case and the legal consequences of various articles of the GDPR. The students had a professional background on data privacy and security and attended an extra-occupational education class on workflow modeling.

The students have observed that the general criteria for the applicability of the norm (1a) refer to domain knowledge of the workflow that cannot be easily represented as a check list or a BPMN-style workflow model. We think that describing the criteria textually is the most appropriate option. Furthermore, our students have reported that the set of circumstances for the applicability of a specific article (1b) does not have an inherent order. Therefore it makes no sense to represent the circumstances as a workflow model fragment with a graphical language. A simple check list is sufficient and was preferred by the students. Our students also found out, that the legal consequence (2a) can be represented as workflow model. This model can be defined in a semi-formal language such as BPMN or EPC. If the consequence is a straightforward yes/no-conclusion (2b), this part can be cut down to a simple event 'Processing is lawful'. The final observation of the experiment was, that only such articles can be represented in a proposed way, which do not contain uncertain legal concepts. For example, consider Text 4. It requires legal expertise to decide for each workflow instance individually if the interests of the controller are overridden by the rights of a person.

Text 4 (Frag. of Art. 6 GDPR): Lawfulness of processing

> *1. Processing shall be lawful only if (...)*
> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (...)*

IV. The CCC Model

In this section, we introduce our CCC model. It structures fragments of legal texts into Context, Condition and Consequence. In the previous section, we have observed a similarity between the general structure of legal texts (the circumstances for applicability of an article, the legal requirements named in the article and the legal consequence) and three basic elements of a pattern (context, problem, solution). This similarity is outlined in Figure 3. Furthermore, we have obtained evidence how the different parts of legal texts can be represented. In this section, we first describe elements of a WPP structure, and then follow up with the CCC Model, which describes how to obtain systematically WPPs from legal texts.

A. WPP structure

We aimed for WPP structure elements that mirror and foster desirable characteristics of design patterns, such as completeness, understandability and reusability (Requirement R1). Furthermore, the structure of a WPP shall carry all legal obligations from the data privacy domain for a given scope (Requirement R2). It shall not result in oversized, inapplicable pattern forms, that violate the Requirement R1. The structure must allow modular stacking of WPPs (Requirement R3). Considering this, our WPP structure consists of *Header, Context, Condition* and *Consequence*:

a) Header: The header contains meta-information of the pattern. It describes essentials like name, type, legal focus of the WPP and relation to other WPPs. Further meta-information as an unique database ID, date or the name of the WPP creator, may be added.

WPP Name A distinct name of the pattern. It makes the pattern easily recognizable, and allows searching for it in a pattern catalog. The name of the WPP shall indicate the objective of the pattern.

WPP Type WPPs can be distinguished into check patterns and activity patterns, as observed in the last section.

Legal Focus Specifies all legal texts (articles, paragraphs, etc.) which were used to derive the pattern. It declares which legal obligation is covered (entirely or partly) with this WPP.

Relation to other WPPs WPPs can build upon each other. When implementing multiple WPPs into a workflow, sometimes the relation between WPPs needs to be specified. For example, a WPP creator might decide to split the legal obligation to delete data into multiple WPPs. One WPP keeps records of the data used, a second one ensures that the data is deleted at the specified time. WPPs might also exclude each other. For example, a WPP to execute a business task anonymously might exclude a WPP for the deletion of personal data. Since new WPPs might be created at any time, information on the relation to other WPPs may be incomplete.

b) Context: The context of a WPP contains an intuitive textual description of the situation and of the resulting problem, which is addressed by the WPP. The user must clearly understand when and for which objectives the WPP can be applied, and if the application of the WPP results in further legal obligations.

c) Condition: The condition provides all prerequisites mentioned in the legal texts that have been enumerated in the 'legal focus' field of the WPP header. Since the order of the prerequisites is insignificant, the condition is represented as a checklist. The prerequisites have to be defined as positive statements that do not leave room for misunderstanding. If all prerequisites in the checklist are met, the consequence applies.

d) Consequence: The consequence of a check pattern is a statement, which is true, if all prerequisites from the condition are fulfilled. In order to determine the consequence of the WPP, it is necessary to specify the type of the pattern first. This is, because the consequence component differs in its form depending on the type of the WPP. For a check pattern it is (a) a statement that the case described in the context field is lawful, according to the legal norms specified in the header. Alternatively - for an activity pattern - the consequence is (b) a chain of activities, specified with a workflow modeling notation like EPC (event-driven process chain) or BPMN (Business Process Model and Notation). This chain of activities has to be executed, if all the prerequisites described in condition component are met.

B. The CCC Model

Typically, modeling a new WPP is triggered by a workflow engineer or a privacy officer, who has identified a recurring, challenging problem which has no corresponding pattern. Recall that the WPP creator must be familiar with legal texts (Requirement R2), but the workflow engineer does not necessarily possess such knowledge. Thus, a model for deriving WPPs must ensure, that all legal obligations are included in the resulting WPP.

We will now outline the six steps needed to derive a WPP. They constitute our CCC Model. For this we use the structure described in previous subsection. We use Text 1 to illustrate these steps. Note that Text 1 refers to an activity pattern. An example for a check pattern can be found in the Appendix.

a) Define the Scope: At first, the WPP creator sets the outline of the new WPP. He decides which legal articles and paragraphs will be in the scope. By setting the scope, he must ensure that the resulting WPP meets the requirements of design patterns (R1). In particular, the WPP must be not too complex or too simple to be useful. He also has to ensure that the new WPP can be combined with already existing WPPs (R3). Furthermore, the WPP creator has to consider that the legal texts in the scope do not contain uncertain legal concepts that are unsuitable for a WPP, as shown in Text 4. Scoping of a WPP can be supported with four questions:

- Is the scope suitable to create a WPP that is non-trivial?
- Is the scope understandable for the workflow engineer?
- Does the scope overlap with a WPP that already exists?
- Does the scope include legal texts that need to be interpreted individually by a legal expert?

Example 1: The scope of the WPP is the implementation of the 'right of access' according GDPR for customer data. The company doesn't collect data from and doesn't transfer data to third parties, but it uses automated means for data processing of customer data in the EU. Furthermore, the WPP addresses only requests that arrive electronically.

b) Define the Header: In this step, the meta-data of the WPP is defined. The meta-data of the pattern is the *Name*, the *Type*, the *Legal focus* and the *Relations to other WPPs*. The WPP name should be intuitively understandable and reflect the WPP type. A name beginning with 'Processing' would indicate an activity pattern, while a name starting with 'Lawfulness of' would refer to a check pattern.

The articles and paragraphs specified in 'Legal Focus' mirror the scope of the WPP. 'Relations to other WPPs' contains information if the scope of this WPP depends on, overlaps with or contradicts with existing WPPs.

Example 2:
WPP Name *Processing the Right of Access from the Inventory of Processing Activities*
WPP Type *Activity Pattern*
Legal Focus *Art. 15 Par. 1a-d, Par. 3; Art. 2 Par. 1; Art. 3 Par. 1 GDPR*
Relation to other WPPs *dependency to WPP 'Update Inventory of Processing Activities'*

c) Define the Context: In the third step, the context must be specified. It shall describe the situation and the purpose of the pattern in a plain language that is clearly understandable without legal expertise. It must provide answers for the following questions:

- Which business activities are in concern of this WPP?
- When does the privacy pattern apply?
- Which activities can occur before or after the WPP?

Example 3: A business unit has received a request from a customer. The customer asks if personal data concerning him is processed. If this is the case, the customer must be given access to his personal data.

d) Define the Condition: The condition translates legal requirements into prerequisites for the applicability of a WPP. The prerequisites have to be defined as positive statements that do not leave room for misunderstanding for a person without legal expertise. Thus, we discourage citing or referring to legal texts. The following questions serve as a guideline to to obtain a check list of conditions:

- Which legal texts are in the 'Legal Focus' of this WPP?
- Do those texts base on other legal definitions?
- Which different requirements exist in each sentence of the legal text?
- Is a certain requirement already excluded by 'Context'?

Example 4:

- ☐ *The identity of the requester has been verified.*
- ☐ *The requester asks for his or her own data.*
- ☐ *The requester does not make use of this right more than three times a year.*

e) Define the Consequence: The Consequence depends on the WPP type. For a check pattern only a state must be defined, which comes into effect when all requirements set in the Condition are met. For an activity pattern, the consequence is a chain of activities which must be specified (e.g. in form of an EPC notation) in this step.

Example 5: Figure 4 describes the activities to process the request for access from a customer as a business process model.

f) Review the WPP: To ensure that the pattern is correct and useful, it must be reviewed according to the following questions:

- Does the WPP meet the general quality criteria of design patterns?
- Is the WPP understandable and applicable for persons without legal expertise?
- Do the components Context, Condition and Consquence represent all information specified in the 'Legal Focus'?

C. Discussion

We have derived our WPP representation from the general structure of legal texts. Essentially, we can represent any legal article (or its fragment) as a WPP. However, it was not in the scope of this paper to find out if a WPP representation makes sense for a certain use case. For example, Article 21 GDPR contains "legitimate grounds for the processing which override the interests, rights and freedoms of the data subject". It needs a lawyer to find out if such grounds indeed override the rights of the subject. If a WPP contains such concepts, it might not be useful for a workflow engineer, who does not possess legal expertise. But it might possible to decide upon such aspects at the creation time of the WPP. Thus, we see potential for further research.

It remains an open issue to evaluate our approach systematically. This is challenging: we have to consider three distinct user roles, with specific expertise areas and domain knowledge. It is difficult to separately assess the WPP representation and the framework for generating this representation. It is also challenging to exclude the properties of the application domain, when testing the applicability of a WPP. For this reasons, we plan to evaluate our approach with a broad, qualitative case study.

Finally, it needs to be investigated how the creation, usage or verification of WPPs can be supported within workflow modeling tools or even within workflow modeling notations. Furthermore, corresponding frameworks and (semi-)automatic approaches would help to express the full potential of the WPPs. They could support the verification if the workflow embeds a WPP correctly. They also could help confirming if the WPP is conclusive, that is, if all (or particular) aspects of a certain legal text are represented within the WPP.

V. Conclusion

The GDPR and other privacy norms resulted in new requirements for workflows that handle personal data. It may be - for example - a requirement to ensure that a particular information is used only for the purpose explained to the customer. This information must be deleted when the original purpose for which it was gathered is no longer valid. Furthermore, individual rights such as the 'right of access' or the 'right to be forgotten' require for new workflow extensions which are not directly related to the original core business objectives of a company.

Implementing privacy norms into workflows is challenging. Auditors, workflow engineers and data privacy officers normally have different fields of expertise, but must cooperate in an interdisciplinary way to implement or verify legal requirements in domain-specific business tasks. A promising approach to tackle such challenges is the use Workflow Privacy Patterns (WPPs). WPPs provide solutions to problems recurring in enterprise workflows. However, existing work on WPPs does not explain how such patterns can be obtained in a systematic way.

In this paper, we have investigated how to derive WPPs from legal texts such as the GDPR. We have defined three distinct user roles that are involved in the creation and use of WPPs. Furthermore, we have compared the characteristics of legal texts with the properties of design patterns. From this point we have developed a formal representation of WPPs that follows the structure of legal norms. Furthermore, we have developed a framework that compiles WPPs in six steps. With two different use cases we have provided evidence that our approach allows to map articles of the GDPR into a formal representation which supports process engineers in designing workflows, which meet legal requirements.

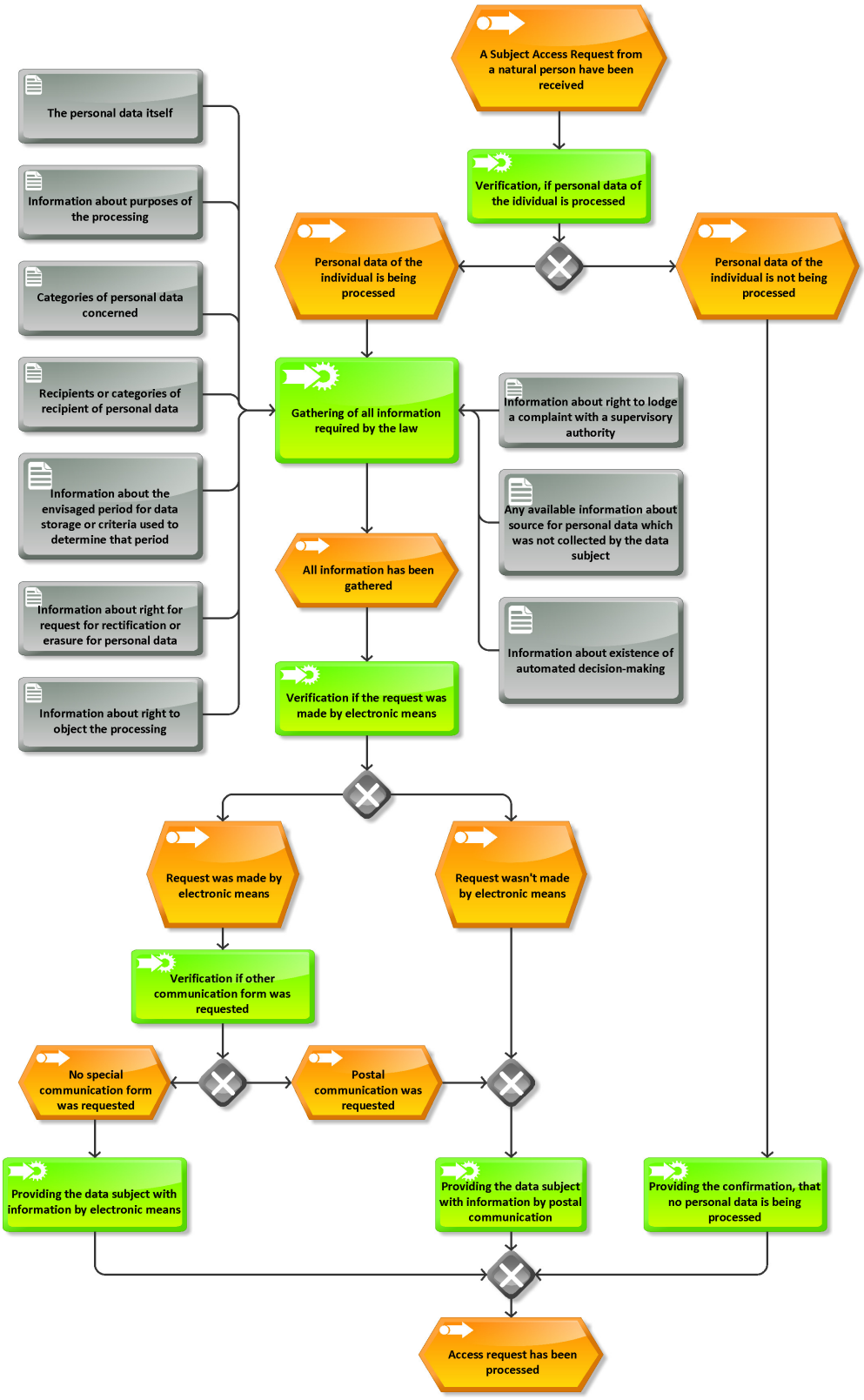

Fig. 4. Workflow to handle a request for acccess.

ACKNOWLEDGMENT

We would like to thank Martin Bahr for his exceptional work on realizing the CCC Model.

APPENDIX
EXAMPLE FOR A CHECK PATTERN

In this section, we illustrate a check pattern with the GDPR articles related to the consent for data processing. In particular, we have used our approach (cf. Section IV) to develop a WPP for the lawfulness of an electronic consent.

a) Scope:

Before an enterprise processes personal data, it must verify the lawfulness of processing. If there is no other legal basis, say, from other laws or a contract, the data subject must have been provided a consent to the processing of his or her data. The purpose of this WPP is to prove the lawfulness of an electronic consent from an adult according to the GDPR. The consent has been documented in a database.

b) Header:

WPP Name Lawfulness of an electronic consent
WPP Type Check pattern
Legal Focus The WPP considers the GDPR articles:

- Art. 4 ('definitions'), Par. 11 ('consent')
- Art. 6 ('lawfulness of processing'), Par. 1 (a)
- Art. 7 ('conditions for consent')

Relation to other WPPs

- 'Obtain Electronic Consent'
- 'Revoke Electronic Consent'

c) Context:

The purpose of this WPP is to prove the lawfulness of an electronic consent from an adult for the processing of personal data for a specific purpose.

d) Condition:

- ☐ There exists a record of a consent from the data subject in the database.
- ☐ The consent has been obtained in a lawful way. (cf. WPP 'Obtain Electronic Consent')
- ☐ The record documents that the data subject has been informed about processing activity, data to be processed, purpose of the processing, storage period, parties responsible for the processing and the receivers of the data.
- ☐ The record corresponds to the current processing.
- ☐ In the last 18 months, the consent has been given or there has been a processing activity related to this consent.
- ☐ There is an option to withdraw the consent that is easily accessible for the data subject. (cf. WPP 'Revoke Electronic Consent')
- ☐ The consent has not been withdrawn.

Note that the GDPR does not specify an expiration period for a consent. However, court decisions say that it is best practice not to rely on a consent that might have been forgotten already by the data subject.

e) Consequence:

If all conditions are fulfilled, a lawful consent for the processing exists.

REFERENCES

[1] European Parliament and Council of the European Union, "Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," EU Regulation 2016/679, 2016.
[2] E. Buchmann and J. Anke, "Privacy patterns in business processes," *INFORMATIK 2017*, 2017.
[3] R. Von Alan and R. Hevner, "Design science in information systems research," *MIS quarterly*, 2004.
[4] P. Schaar, "Privacy by design," *Identity in the Information Society*, vol. 3, no. 2, pp. 267–274, 2010.
[5] Information Commissioners Office, "Guide to the general data protection regulation (gdpr)," https://ico.org.uk, Accessed Jul., 2018.
[6] C. Alexander, *A pattern language: towns, buildings, construction*. Oxford university press, 1977.
[7] P. Wolfgang, "Design patterns for object-oriented software development," *Reading Mass*, vol. 15, 1994.
[8] D. C. Schmidt, M. Stal, H. Rohnert, and F. Buschmann, *Pattern-Oriented Software Architecture, Patterns for Concurrent and Networked Objects*. John Wiley & Sons, 2013, vol. 2.
[9] A. Ter Hofstede, B. Kiepuszewski, A. Barros, and W. Aalst, "Workflow patterns," *Distributed and Parallel Databases*, vol. 14, no. 1, pp. 5–51, 2003.
[10] S. Jablonski and C. Bussler, *Workflow management: modeling concepts, architecture and implementation*. International Thomson Computer Press London, 1996, vol. 392.
[11] N. Russell, W. M. van der Aalst, and A. H. M. ter Hofstede, *Workflow Patterns: The Definitive Guide*. MIT Press, 2016.
[12] N. Russell *et al.*, "Workflow control-flow patterns: A revised view," *BPM Center Report BPM-06-22, BPMcenter. org*, pp. 06–22, 2006.
[13] ——, "Workflow data patterns: Identification, representation and tool support," in *International Conference on Conceptual Modeling*. Springer, 2005, pp. 353–368.
[14] ——, "Workflow resource patterns: Identification, representation and tool support," in *International Conference on Advanced Information Systems Engineering*. Springer, 2005, pp. 216–232.
[15] ——, "Workflow exception patterns," in *Conference on Advanced Information Systems Engineering*, 2006.
[16] B. S. Lerner *et al.*, "Exception handling patterns for process modeling," *Transactions on Software Engineering*, vol. 36, no. 2, 2010.
[17] EU FP7 Project PRIPARE, "privacypatterns.eu - collecting patterns for better privacy," https://privacypatterns.eu, Accessed Apr., 2019.
[18] Projects by IF, "Data permissions catalogue - an evolving collection of design patterns for sharing data," https://catalogue.projectsbyif.com/, Accessed Jun., 2019.
[19] J. Vom Brocke, *Design principles for reference modeling: reusing information models by means of aggregation, specialisation, instantiation, and analogy*. IGI Global, 2007.
[20] F. Buschmann, K. Henney, and D. C. Schmidt, *Pattern-oriented software architecture, on patterns and pattern languages*. John wiley & sons, 2007, vol. 5.