Privacy Patterns in Business Processes

Erik Buchmann[1] and Jürgen Anke[2]

Abstract: Workflow design patterns provide abstract, „best-practices" solutions to recurring problems. While the majority of workflow patterns focus on control flow, resources and data, our concern are patterns from a data privacy perspective. Privacy patterns have the potential to ease the life of process developers, auditors and privacy officers by providing pre-validated patterns that correspond with existing data privacy regulations. With this paper, we strive to establish workflow privacy patterns as a direction of research. For this purpose, we motivate privacy patterns, we discuss requirements and research directions, and we review options to integrate patterns into existing modeling languages and tools.

Keywords: GDPR; Privacy Modelling; Business Processes; Workflow Pattern

1 Introduction

Design patterns are reusable solutions to a commonly occuring problem. By instantiating a design pattern, an engineer can arrive at a „best-practices"-solution with little effort. In the area of workflow modeling, a large number of workflow design patterns have been proposed [tH10, RvdAtH16]. A prominent example is „Multiple Instances Without Synchronization". This pattern creates a number of identical, independent sub-processes whose number is unknown at design-time. However, the majority of workflow patterns focus on the perspectives „Control Flow", „Data" and „Resources". In contrast, our focus is on the *Data Privacy Perspective*, which allows to verify the compliance of processes with privacy laws, with binding corporate rules or with the privacy policy of an enterprise. This perspective also helps to realize data minimality and privacy-by-design, to implement fundamental activities that involve the privacy officer into sensible processes, etc. In this paper, we outline workflow privacy patterns (WPP) as a research area. To this end, we motivate the use of workflow patterns for the data privacy perspective and name requirements for WPPs that are useful in practice. Furthermore, we review options to instantiate WPPs in modeling languages and modeling tools, and we discuss directions for future research on WPPs.

The next section reviews related work. In Section 3, we introduce the various aspects of privacy patterns. Section 4 discusses research directions and concludes this paper.

[1] Hochschule für Telekommunikation Leipzig, Germany, buchmann@hft-leipzig.de

[2] Hochschule für Telekommunikation Leipzig, Germany, anke@hft-leipzig.de

doi:10.18420/in2017_79

2 Related Work

Some software design patterns for data privacy concepts [EU17] already exist, while workflow patterns have attracted less attention. Here, we review related work on the topic.

Workflow Patterns: Workflow models consider different perspectives[JB96], depending on the latter use of the model. Well-known perspectives are the „Control Flow", „Data", „Resources", „Functional" and „Operational". Most workflow patterns [tH10, RvdAtH16] focus on the first three perspectives. For example, [RHM06] lists 43 different patterns ranging from general sequences to the explicit termination of processes. [RvdAtH06, Le10] presents exception handling patterns. [WRRM08] focuses on patterns for control-flow changes. Patterns on the data perspective [Ru04a] consider the visibility of data, data-driven interactions, the transfer of data and its transfer routes. Patterns such as „Role-based Allocation" [Ru04b] address the life cycle of work items from the resources perspective.

Data Privacy Legislation: Data privacy laws regulate the collection, management, storage and transfer of personal data. To ease the transborder flow of data, international efforts such as the „OECD Privacy Framework" [OE17], „Binding Corporate Rules" [Ar09] or the „EU General Data Protection Regulation" [EC16] harmonize national privacy regulations. Thus, WPPs exist that abstract from national privacy laws. Such WPPs might facilitate the adaption of privacy rules to enterprise processes and ease the verification of processes towards privacy. Such a concept for security in workflows has been described already [AMF15].

Privacy in Workflows: Since privacy legislation regulates the handling of (person-related) data by (human) resources, some patterns from the perspectives „Data" and '"Resources" are related to data privacy. One example is the pattern „Separation-of-Duties" [Ru04b], which realizes the four-eye-principle. It can also ensure that a business entity cannot generate personality profiles. Another one is „Scope Data" [Ru04a], which limits the visibility of data and can implement the principle of purpose. An orthogonal option to integrate privacy is extending modeling languages by annotations [MvSB11]. However, this approach cannot express generalized patterns independent from a particular modeling language. Finally, [Ar16] identifies patterns that link organisational privacy goals to process models. However, organisational goals result in patterns on a high level of abstraction, e.g., „Data Protection" or „Unlinkability", which are difficult to transform into concrete process models.

3 Privacy Patterns in Workflows

In this section, we discuss how WPPs materialize in processes and how to integrate them into the existing tool-chain. We start by providing an intuitive WPP example:

Privacy Pattern: ***Anonymous Access Path***

Description: *A given service process can be executed either anonymously or personalized. Thus, the customer needs to be informed about the alternatives and must decide upon providing personal data or not. Providing personal data is an implicit consent.*

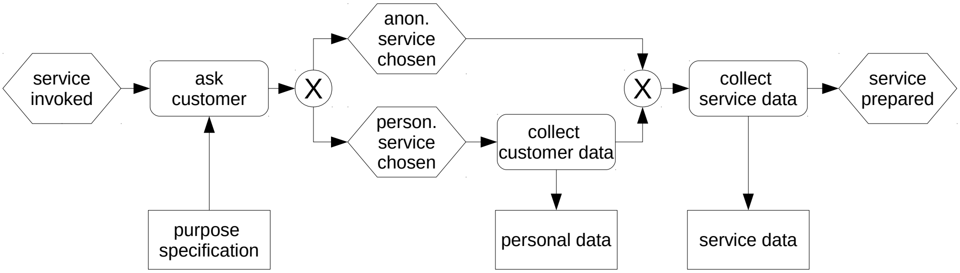

Abb. 1: Anonymous access path (Event-driven process chain)

Solution: *A preceding sub-process (see Figure 1) allows the customer to chose between anonymous or personalized service. In the latter case, an activity fetches personal data.*

Legal Requirements: *The activity „Ask Customer“ must inform the customers about the consequences of providing personal data. In particular, the customer must been told which data is collected, to which purpose the data is used, if data is transferred to 3rd parties etc.*

Privacy Processes: *Update Directory of Procedures; Notify Privacy Officer*

Related Patterns: *Personalized Access with Explicit Consent*

3.1 WPPs in Process Models

We have observed three distinct ways how data privacy must be considered in workflows:

Privacy Processes: First, implementing data privacy into the enterprise IT results in processes of its own: As a result of the current data privacy legislation [EC16], each enterprise that handles personal data must implement a number of workflows. For example, the individual concerned must be able to find out which personal information is stored by the enterprise, and it must be able to request a correction or deletion of personal data. If the individual has given consent to the processing of personal data, the consent must be stored and it must be possible for the individual to revoke its consent at any time.

Crosscutting Privacy Patterns: Second, data privacy is a crosscutting concern for all processes that handle personal data. For example, any process that handles personal data must validate a number of criteria that are required by legislation: Is the process sufficiently announced in the privacy policy of the enterprise? Is it mandatory to inform the individual concerned about processing activities at certain points in the workflow? Must the individual give consent to the processing of data? Does a previously given consent to a privacy policy allow to execute a certain workflow? Those privacy concerns result in building blocks that must be mounted in a similar way at multiple places into the process models.

Meta Privacy Processes: Third, concepts such as the separation-of-duty, separation-of-concerns, un-linkability of data, data minimality or privacy-by-design have a direct effect on the process design, even if no activity in the process directly relates to privacy. For example, separation-of-duty protects the privacy of an individual by enforcing that different tasks are executed by different roles so that no single person in the enterprise is able to obtain an in-depth profile of the individual concerned. The implementation of such concepts require meta processes whose building blocks are materialized in processes such as IT-demand management, requirements engineering, IT operations and IT development.

3.2 Putting WPPs into Practical Use

WPPs have to provide a clear benefit over the manual modeling privacy in processes. Thus, it must be as intuitive as possible to apply WPPs for a process designer, both from the perspective of the tools used and from the perspective of the modeling language. Furthermore, the abstract representation of privacy patterns must add value over recycling process fragments that have been modeled earlier. We have derived three main requirements for the concept of privacy patterns:

(R1) *WPPs should not require modifications of the chosen modeling language.* Existing modeling languages have been developed and taught over years, they have been implemented in modeling and simulation environments, and there is a wide body of literature on transformation rules, verification concepts etc. Thus, it should generally be avoided to extend a modeling language for privacy pattern support.

(R2) *WPPs should be useful for both the process modeling and implementation.* Privacy patterns are particularly beneficial if they integrate well into the existing toolchain, from development over simulation/validation to the process execution. Thus, privacy patterns must be specified on a level of abstraction that can be readily implemented.

(R3) *WPPs should be able to be maintained separately from the actual business processes.* Various privacy-related aspects have been changed recently, be it due to the cancellation of the Safe-Harbor treaty, be it due to the attempts to establish a data retention directive. Thus, it would be beneficial to update all processes at once if a privacy pattern has been updated.

As modelling languages provide different possibilities for extensions, refinements or modularity in general, this affects the practical handling of WPPs. Furthermore, not all languages features might be supported by all tools for that language. The same language could provide different capabilities in different versions. Hence, we need to consider the combination of modelling language, language version and used modelling tool to identify potential mechanisms for provisioning privacy patterns. In general, we see three strategies to integrate WPPs into existing modeling tools.

Integration into a process template library: Each sophisticated modeling tool comes with a user-extensible library for process fragments. Integrating WPPs into such a library does not require changes on the tools or the language (R1). Tools usually copy patterns from the library into a model designer tool (R2). However, there is no option to update processes by modifying patterns (R3).

Extending stateful modeling languages: Languages such as extended Petri nets allow typed tokens that represent process states. It would be possible to define privacy types orthogonally to existing types and let privacy activities react on them. For example, the type of a token could carry the information that a customer has consented to a certain activity, parallel to the state of the activity (R1). However, this would inflate the number of types, making the model difficult to understand and to implement (R2). Finally, the privacy patterns would have to be compiled into specialized activites, which is in conflict with R3.

Using preprocessors or aspect-oriented approaches: A third approach is to use a preprocessor or to „weave“ privacy patterns into processes using concepts from aspect-oriented programming. For example, AO4BPEL [CM06] provides a BPEL-process weaver [SV08] which integrates crosscutting concerns into process models. This approach supports the requirements R2 and R3, but it is in conflict with R1.

Since none of these strategies fulfills all of our requirements, we see a clear demand for further research regarding the integration of WPPs into modeling languages and tools.

4 Conclusions and Outlook

We have motivated the benefits of privacy patterns, and we pointed out connections to existing concepts and to requirements for privacy patterns that are useful in practice. Workflow design patterns provide well-tested and well-researched concepts to solve recurring problems. While many patterns have been proposed, the research on workflow patterns for data privacy concepts is just at the beginning. Amongst a large number of open research questions, we deem the following ones to be most important:

Which WPPs are refinements of processes or cross-cutting concerns? This impacts the mechanisms that can be used to integrate the in both languages and tools. While refinements are a concept in process modelling, cross-cutting concerns are a concept of aspect-oriented programming and thus address the implementation level.
How can WPPs be modelled independently of concrete modelling language? Here, we aim to provide WPPs in a way that can be used in multiple modelling languages, e.g. BPMN and UML activity diagrams. A promising candidate might be Petri nets.
How can we provide support for multiple modelling languages and tools? For that, we need to investigate the possibilities for the formal integration in the languages as well as the technical integration in the tools.

While our work is in an early stage, we are conviced that any contribution for the integration of privacy support in business process are highly relevant for both research and practice.

Literaturverzeichnis

[AMF15] Argyropoulos, N.; Mouratidis, Haralambos; Fish, Andrew: Towards the Derivation of Secure Business Process Designs. In: Conference on Conceptual Modeling. 2015.

[Ar09] Article 29 Data Protection Working Party: , Working Document on Frequently Asked Questions related to Binding Corporate Rules. Working Document WP 155, 2009.

[Ar16] Argyropoulos, N. et al.: Incorporating Privacy Patterns into Semi-Automatic Business Process Derivation. In: Conf. on Research Challenges in Information Science. 2016.

[CM06] Charfi, Anis; Mezini, Mira: Aspect-Oriented Workflow Languages. In: OTM Confederated International Conferences. 2006.

[EC16] European Parliament; 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.

[EU17] EU FP7 Project PRIPARE: , privacypatterns.eu - Collecting Patterns for Better Privacy. https://privacypatterns.eu, Accessed Apr., 2017.

[JB96] Jablonski, Stefan; Bussler, Christoph: Workflow Management: Modeling Concepts, Architecture, and Implementation. International Thomson, 1996.

[Le10] Lerner, B. S. et al.: Exception Handling Patterns for Process Modeling. Transactions on Software Engineering, 36(2), 2010.

[MvSB11] Mülle, Jutta; von Stackelberg, Silvia; Böhm, Klemens: Modelling and Transforming Security Constraints in Privacy-Aware Business Processes. In: Conference on Service-Oriented Computing and Applications. 2011.

[OE17] OECD: , The OECD Privacy Framework. http://www.oecd.org, Accessed Apr., 2017.

[RHM06] Russell, Nick; Hofstede, Arthur H. M. Ter; Mulyar, Nataliya: Workflow Control-Flow Patterns: A Revised View. Bericht, BPM Center Report BPM-06-22, 2006.

[Ru04a] Russell, Nick et al.: Workflow data patterns. Bericht, Queensland University of Technology, FIT-TR-2004-01, 2004.

[Ru04b] Russell, Nick et al.: Workflow resource patterns. Bericht, BETA Working Paper Series, WP 127, 2004.

[RvdAtH06] Russell, Nick; van der Aalst, Wil; ter Hofstede, Arthur: Workflow Exception Patterns. In: Conference on Advanced Information Systems Engineering. 2006.

[RvdAtH16] Russell, Nick; van der Aalst, Wil M.P.; ter Hofstede, Arthur H. M.: Workflow Patterns – The Definitive Guide. MIT Press, 2016.

[SV08] Sánchez, Mario; Villalobos, Jorge: A Flexible Architecture to Build Workflows Using Aspect-Oriented Concepts. In: AOSD workshop on Aspect-Oriented Modeling. 2008.

[tH10] ter Hofstede, Arthur H. M. et al.: Modern Business Process Automation: YAWL and its Support Environment. Springer-Verlag, 2010.

[WRRM08] Weber, Barbara; Reichert, Manfred; Rinderle-Ma, Stefanie: Change Patterns and Change Support Features. Data & knowledge engineering, 66(3):438–466, 2008.