Patterns in Privacy - A Pattern-Based Approach for Assessments

Jörn Kahrmann, Ina Schiering

Patterns in Privacy - A Pattern-Based Approach for Assessments

Jörn Kahrmann[1] and Ina Schiering[2]

[1] joern.kahrmann@ostfalia.de
[2] i.schiering@ostfalia.de

Abstract. The concept of patterns was first developed in the context of architecture and is now widely used in different fields such as software design or workflow design. In the last years the idea of patterns is also used to incorporate privacy in the life-cycle of Information Technology (IT) services. Concerning privacy and security, patterns are mainly used in the design phase of IT services in the form of design patterns. In this paper we propose a pattern-based approach to assess the compliance with privacy regulations continuously during the operation phase of an IT service. The central idea of patterns in this area is to provide an abstract representation of typical automated processing procedures for the processing of personal data. Since these patterns represent abstracted versions of workflows, we use as an illustration diagrams with a notation derived from Business Process Management Notation (BPMN). The aim of the approach presented here is to increase the transparency of assessments for all participants and to allow an easy adjustment of existing assessment results when changes occur.

Keywords: assessment, BPMN, compliance, IT service, pattern, privacy

1 Introduction

Patterns are an important concept in computer science which is widely used especially in the design phase of the software development life-cycle. Beside the very generic design patterns of e.g. Gamma et al. [1], there are also approaches for design patterns in the area of security, privacy, and patterns for workflows. These approaches are described in Section 3.

In the approach presented here, a concept of patterns is proposed that facilitate assessments concerning the compliance with privacy regulations during the operations phase of IT services. In this context patterns represent abstract versions of workflows with hints concerning typical weaknesses encountered in practice. The potential weaknesses can be used as hints during the interviews of an assessment. Hence processes in organisations that are supported by IT services can be assessed continuously for potential weaknesses. The concept of patterns for assessment is presented in Section 4. Since the concept of patterns presented here is more related to the concept of workflow patterns, the definition

of patterns used as a basis in this paper is the definition used also by van der Aalst et al. [2] in the context of workflow patterns. They based their considerations on the definition proposed by Riehle et. al. [3] "A pattern is the abstraction from a concrete form which keeps recurring in specific non-arbitrary contexts."

The approach of pattern-based assessments was developed in the project "Datenschutz-Cloud". The concept of patterns as described above is used as a basis for tool-based assessments with a focus on small and medium sized companies (SMEs). The general architecture is presented in Section 5 followed by a description of assessments that are based on the tools developed during the project in Section 6. The technical solution is described in more detail in [4]. Here the focus is on the underlying concept of patterns for assessment.

Since the project has to adhere to German Data Protection Law [5], we have derived our patterns mainly from the German Federal Data Protection Act (BDSG) and other national laws. Still the patterns are not limited to a German scope since data protection law in European Member States is harmonized via the European Data Protection Directive 95/46/EC [6]. In the near future a General Data Protection Regulation (GDPR) [7], currently under discussion, will have direct effect on data protection in the Member States. This may lead to some refinements of our patterns, but the changes in the European data protection framework won't require major changes in our approach.

The aim of the use of pattern as a basis for assessment is to provide transparency in interviews and to support experienced data protection officials in the sense of the BDSG [5] by an effective representation of the central elements of data privacy assessments. The motivation is to provide a compromise between a common thread for the interviews of the assessments and sufficient depth for experienced professionals. The structure, which is based on visualisations of workflows accompanied by a description and hints concerning potential weaknesses, instead of a large amount of questions, also allows adapting the results of the assessment in the case of changes efficiently. This approach is supported by a lightweight tool-set. An overview of existing assessment methodologies and tool support in this area is presented in Section 2.

2 Background for Assessments concerning Privacy

The focus of the approach described here is checking for legal compliance concerning privacy in SMEs by assessments. The basis of the investigation is compliance with the German Data Protection Law. In the following we provide an overview of assessments and tools which are present in this context.

According to the German Data Protection Law [5] "personal data shall mean any information about the personal or material circumstances of an identified or identifiable natural person (data subject)." Typical examples are name, address, telephone number, and information about bank accounts. Concerning SMEs typical personal data is data concerning customers that are natural persons or data about employees.

General principles of German Data Protection Law according to Bizer [8] are

– Lawfulness of data collection, processing and use of personal data
– Consent of the data subject
– Limitation of the purpose
– Necessity concerning the defined purpose and the retention period
– Transparency of data processing for the data subject
– Data Security
– Control of compliance by data protection officials and supervisory authorities

Concerning data security in the Annex to Section 9 of the BDSG, requirements are stated for access control, disclosure control, input control, job control, availability control and separate processing of data collected for different purposes.

According to §4d, §4e BDSG automated processing procedures for personal data must be documented. This is typically realised in the form of a directory of automated processing procedures. Examples of automated processing procedures are payroll accounting, customer relationship management, application procedure, and time reporting of employees.

In §4f BDSG it is stated that private bodies are obliged to appoint a data protection official if at least 10 employees are carrying out the automatic processing of personal data. The data protection official of the company provides access to the directory of automated processing procedures. To create and update this directory, typically assessments are used to assess the compliance of automated processing procedures with privacy regulations, document weaknesses and give advice concerning measurements which should be applied.

Assessments employed for this aim are focussed on checking for the compliance of processes and supporting IT services in the operation phase, i.e. after the initial roll-out or after changes. Examples are the privacy module of IT Grundschutz of the Federal Office for Information Security (BSI) [9] or a variant targeted for SMEs called ISIS12 [10]. For these assessments *verinice*[3] can be used as a tool to manage questionnaires. Beside this there exist other tools like *2B Secure*[4] or *privacyGUARD*[5] which are mainly based on questionnaires. With a focus on cloud services there exists also the tool *CARiSMA* [11] that is based on the risk model of the IT Grundschutz catalogues and uses ontologies to derive questionnaires from legal regulations.

All these assessments and tools intend to give a complete and detailed guideline how to check for weaknesses concerning data privacy and security. That is very important for skill training and to build up experience. But experts in the field tend to derive from their experience a very personal style to conduct interviews. That is a normal development, but it makes it difficult to work in teams with a comparable approach for assessments. Here the intention is to provide an assessment methodology based on patterns that supports experienced data protection officials in the assessment process and proposes a general structure for interviews.

[3] `http://www.verinice.org/`
[4] `http://www.2b-advice.com/`
[5] `http://www.privacyguard.de/`

Another important aspect for data protection officials is to keep track of changes concerning workflows and technologies efficiently. When the initial analysis was based on a large questionnaire it is a complex task to update these initial answers continuously, since a change might have various implications. The model proposed here addresses the adaptation to changes by modelling the status in the form of a graph. In a connected model it is easier to identify implications of changes.

The concept of Privacy Impact Assessments (PIAs), mentioned as Data Protection Impact Assessment in §33 GDPR, has a different focus. A PIA is integrated in the risk management process of projects or the development process of a product. But beside a PIA there are other means needed to check for compliance during the operation phase as referred to in §33 GDPR. The CORAS approach [12], [13] also addresses risk management. It is based on Unified Modelling Language (UML) models, where risks are modelled individually based on the concrete service and its environment. This approach allows also for easy adjustment of models. Whereas the focus of CORAS is modelling of individual risks, the focus of the approach presented in this paper is on checking for compliance. Instead of modelling individual situations, abstract standard models for workflows with typical weaknesses are used in the form of patterns as a basis for all assessments.

3 Existing Pattern Concepts

The idea of patterns was first proposed by Alexander et al. [14] who investigated the use of design patterns in architecture. Gamma et al. transferred these ideas to software engineering [1]. According to Buschmann et al.[15] a design pattern "provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context". In software design, patterns are formulated in the form of Unified Modelling Language (UML) diagrams as an illustration augmented with a documentation consisting of the name, the addressed problem, the solution and consequences. UML diagrams are well understood and lead therefore to transparency and ease of use of patterns. These design patterns are widely used and accepted as guidelines for good software architecture. The patterns are organised typically in the form of a hierarchical structure.

A similar approach is followed by van der Aalst et al. [2] for workflow patterns which are design patterns in the area of workflow design[6]. There petri nets are used as a visualisation accompanied by a documentation with a similar structure as for software design patterns. In a recent approach for design patterns for social applications by Bramilla et al. [16] BPMN is used as a visualisation of social interactions. All these approaches for design patterns organise the patterns in the form of a catalogue which constitutes a hierarchical structure for patterns.

[6] `http://www.workflowpatterns.com/`

There are several approaches to transfer the idea of patterns to the field of security and privacy. There are approaches proposed by Hafiz [17] to formulate Privacy Enhancing Technologies (PETs) in the form of patterns as part of a pattern language for security [18]. Since patterns as "oblivious transfer" and "random wait" are difficult to visualise, patterns in this field consist of a thorough description. The patterns are organised in the form of a hierarchical pattern language, which is an acyclic graph where abstract patterns lead to more concrete patterns. For an overview how privacy design patterns are integrated in the software development life-cycle and incorporated in a system of design strategies see Hoepman [19].

Another approach by Doty and Gupta describes good practices for concrete aspects in the form of privacy patterns[7]. In [20] in addition risks caused by the wrong application of patterns are investigated.

4 Patterns for Assessments

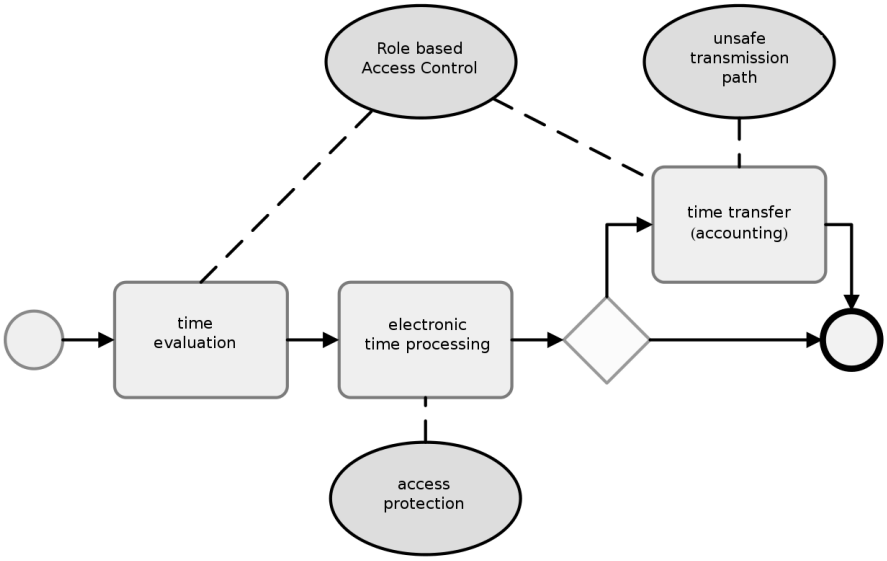

Fig. 1. Time reporting

The definition for patterns, used also in van der Aalst et al. [2], by Riehle et. al. [3] "a pattern is the abstraction from a concrete form which keeps recurring in specific non-arbitrary contexts", is used for the approach of assessment patterns

[7] `http://privacypatterns.org/`

presented here. As a visualisation for abstracted workflows for automated processing operation, a notation based on Business Process Management Notation (BPMN) [21] is adapted.

The patterns for assessment represent abstracted versions of typical workflows, used for automated processing procedures concerning the processing of personal data in the sense of the German Data Protection Law [5]. Instead of modelling individual workflows in organisations, these abstract patterns should be usable in a broad range of situations.

BPMN diagrams of abstract workflows are augmented by information about weaknesses with respect to the activities. Possible weaknesses are denoted in the form of an ellipse that is connected via a dotted line to an activity. Weaknesses can occur at several activities, and several possible weaknesses can be connected to one activity. A description is added to workflows and specific weaknesses. For a proof of concept of the tool-set, automated processing operations of SMEs are used. A typical example is e.g. time reporting of employees performed by an IT service or by a paper based approach (Figure 1).

Another example for an automated processing operation in the sense of BDSG is that companies are obliged to report about the health of employees in the form of a so called health rate (Figure 2). In both examples of patterns there are typical weaknesses proposed, as role based access control is not sufficient, and the transmission path is not sufficiently secured. Concerning the health rate it is important to ensure the anonymity of employees.

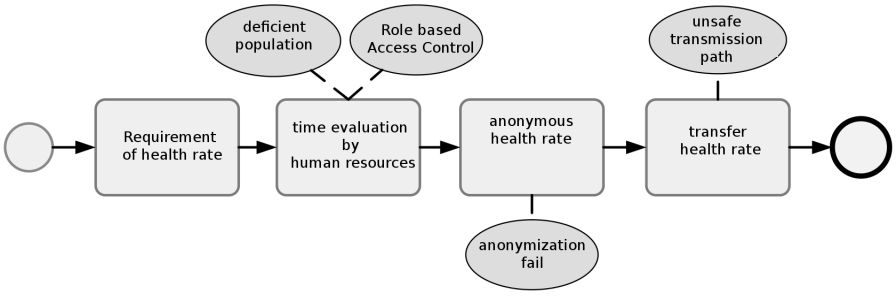

Fig. 2. Health rate

In addition to the automated processing operations, based on the Annex to Section 9 of the BDSG also requirements concerning data security have to be checked during the assessment. There typically a list of aspects have to be ensured. Since these aspects as e.g. access control for buildings or special areas in a building are often not connected to automated processing operations for personal data, a visualisation derived from BPMN diagrams is used with a central activity denoting the area surrounded by several possible weaknesses.

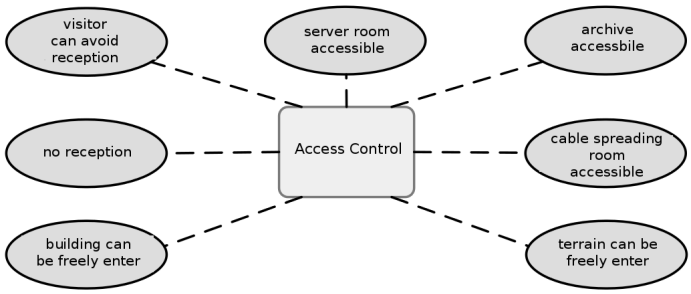

Fig. 3. Access control

These patterns constitute a knowledge pool that can be used for assessment. Patterns are organised in the form of a patterns pool. This is a collection of patterns with a hierarchical structure based on the idea that patterns should facilitate the interviews in assessments. Hence they are ordered by the roles of interview partners and the automated processing procedures they illustrate. Since this collection is not intended to be complete, but to be augmented whenever there are important new variants of processes and IT services, it is called a pool and there is a backend service that allows to add patterns, weaknesses and measurements to this pattern pool.

This pattern pool is integrated in a mobile client as a basis for assessments where weaknesses of specific organisations can be marked and annotated in the representation of the patterns which are used.

After the assessment the result is transferred to a backend service that facilitates the investigation of the assessment result based on the analysis of former assessments and allows the assignment of measurements to the specific weaknesses encountered during the assessment.

5 Architecture

The tool-set that supports the use of the patterns presented above consists of a mobile client for assessments, a web client for the management of the pattern pool and a web client for associating measurements to weaknesses in the graph resulting from the interviews of the assessment. The web clients together with the pattern pool are called the backend of the tool-set in contrast to the frontend which is the mobile client that supports the interviews of the assessment.

The communication between backend and frontend is realised in the form of JavaScript Object Notation (JSON) data structures. The visualisations of patterns are stored and transferred as Scalable Vector Graphics (SVG). The mobile client is an HTML5 client that creates the representation of the assessment dynamically from the JSON data structures representing the pattern pool and if applicable combined with the results of the last assessment.

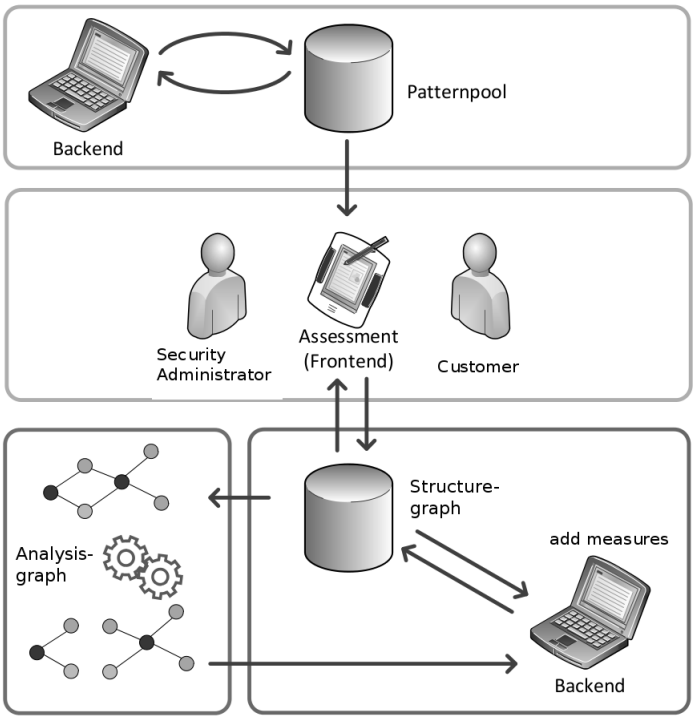

Fig. 4. System overview

The result of the interviews is a data structure consisting of the applicable patterns and the identified weaknesses as nodes. If a weakness is present in a patterns, there is an edge connecting the pattern and the weakness. Hence in the case of common weaknesses like inadequate role based access control it is transparent if the weakness occurs only in special cases or if a general concept is lacking.

6 Tool-Based Assessments

In the following the components of the architecture described above are detailed based on the use cases concerning the pattern pool, the mobile client and the investigation after the interview.

6.1 Modelling Patterns in the Pattern Pool

Weaknesses, measurements and workflows based on automated processing operations can be documented in the pattern pool using a web client in the backend of the IT service. Additional documentation for every element can be added.

First, all needed weaknesses and measurements are added to the pattern pool and connections to possible measurements are connected to weaknesses. Via the pattern editor (see Figure 5) patterns can be created. Beside the BPMN elements only weaknesses which are already documented in the pattern pool can be used in patterns.

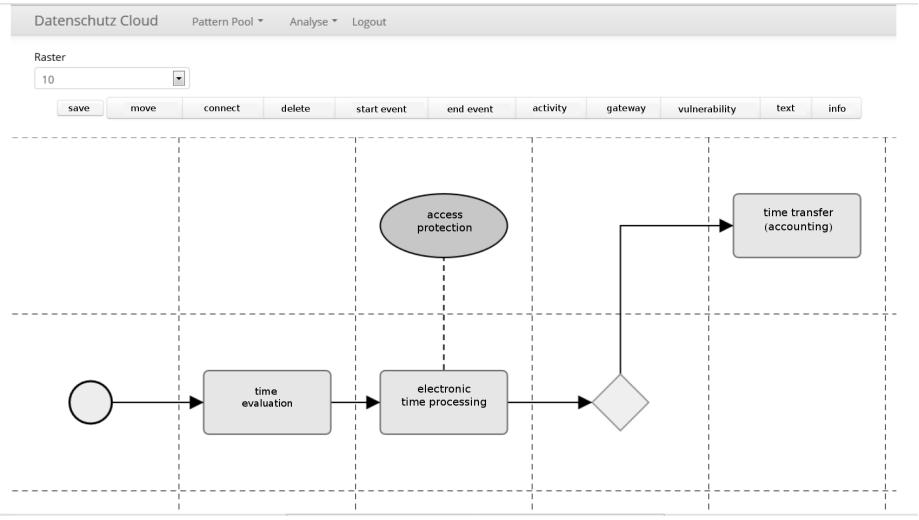

Fig. 5. Editor for pattern pool

For each workflow it is documented further which automated processing procedure, e.g. time reporting, payroll accounting, is represented and what is the role of the intended interview partner concerning this procedure, e.g. management, IT, human resources. These two categories induce a hierarchical structure on the pattern pool. Categories can be added as needed.

6.2 Interviews in Assessment Based on Patterns

To perform an assessment, the actual pattern pool and (if already existent) in addition the result of the last assessment are transferred to a mobile device. The representation of the pattern pool on the mobile device is used as the common thread for all interviews.

After selecting the role of the interview partner, a list of automated processing procedures which are in the responsibility of the role, is presented. If applicable also aspects of data security are included. After choosing an automated processing procedure, a specific pattern can be selected from a list of variants based on the process in the organisation. Since SMEs typically use standard applications and employ relatively simple processes, the list of abstract variants of automated processing procedure according to the experience of the data protection officials

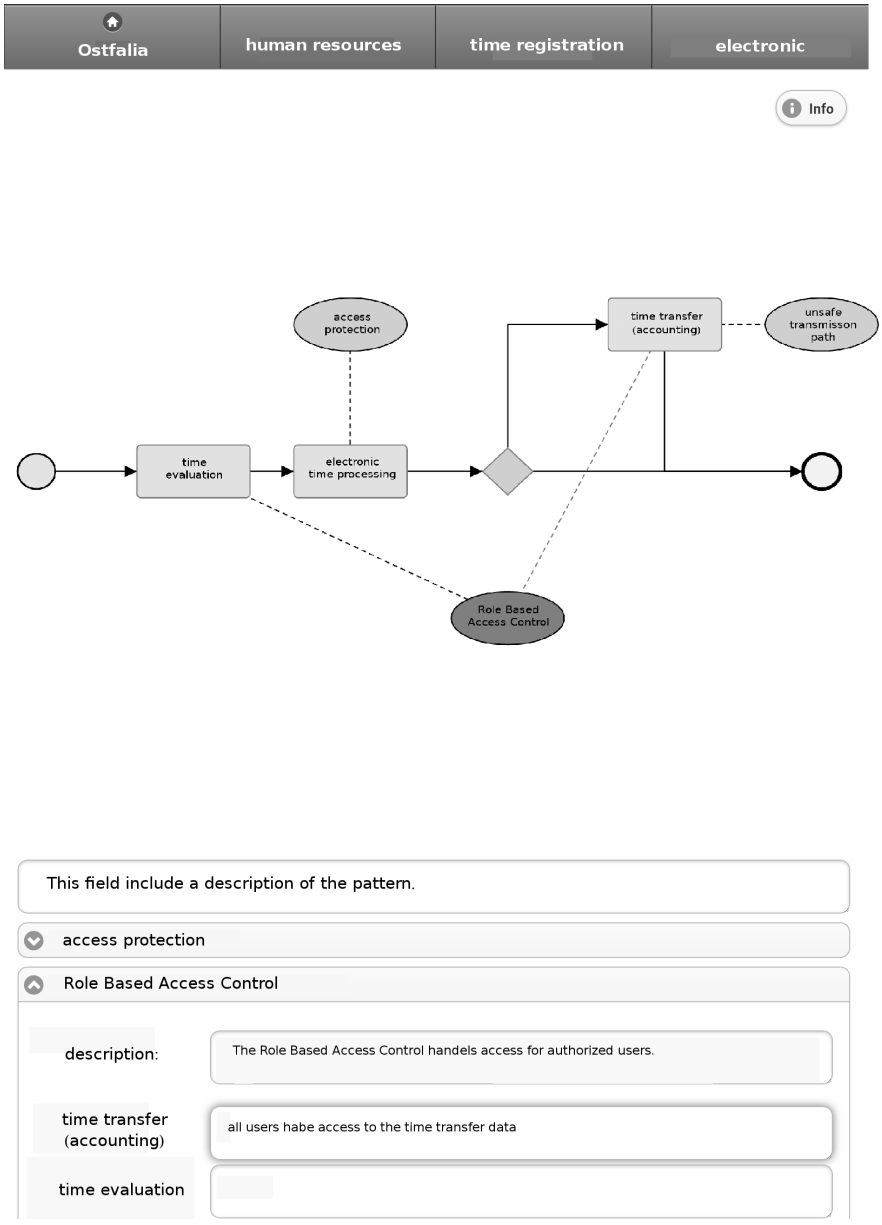

Fig. 6. Client

in the project stays relatively short and an appropriate abstraction for reuse is possible.

Then the pattern as shown in Figure 6 can be used as a transparent basis for the discussion about possible weaknesses. Occurring weaknesses can be selected

in connection with the corresponding activity and are highlighted. Additional notes can be introduced for the pattern in general and each identified weakness.

The mobile client allows an overview which areas are already covered and where weaknesses occurred by marking areas red resp. green.

6.3 Associating Measurements to Weaknesses in the Backend

The result of the assessment consists of the patterns, which describe the processes in the company or considered aspects of data security. In addition occurring weaknesses connected to patterns and activities in the pattern with supplementary notes are integrated. Because a weakness that occurs in several patterns is represented by the same element of the pattern pool, the result is a graph where patterns are connected by common weaknesses.

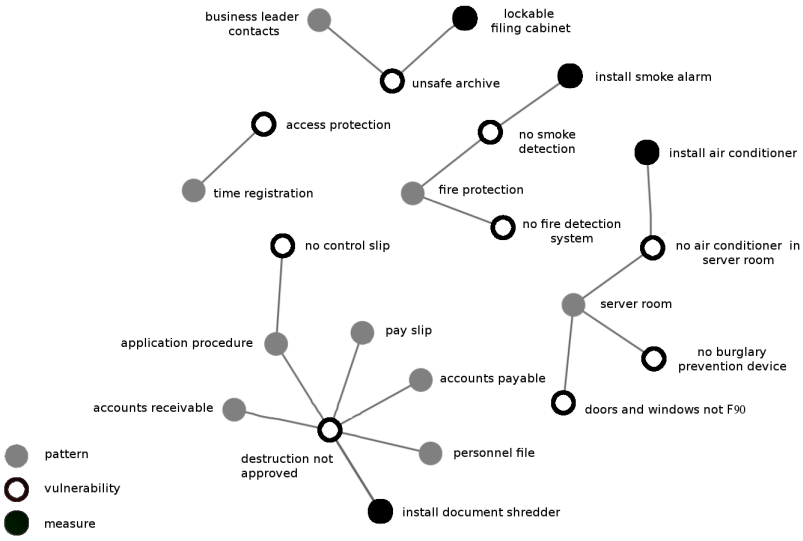

Fig. 7. Overview of results of an assessment with added measurements

This enables the data protection official to get an overview concerning the compliance with privacy regulations. Using a web client in the backend of the tool-set, measurements can be associated to weaknesses from a list of suggestions. The result of the assessment, including the associated measurements, the so-called *structure graph*, is presented in Figure 7.

After the assessment is finished the intention is to generate experience based knowledge from this result without revealing the organisation and specific information about the situation. For this purpose small sub-graphs, so-called analysis graphs, consisting of a weakness with connected patterns and measurements are extracted and stored in a pool of analysis graphs. This knowledge can be used

in the analysis phase of assessments. Suggestions for measurements addressing weaknesses in a specific situation are ranked based on a similarity measurement for analysis graphs. This concept has to be evaluated further, when there is an appropriate number of assessments finalised, such that the pool of analysis graphs is sufficiently large.

6.4 Performing Updates of Assessments

Assessments concerning compliance with legal regulations for privacy need to be updated continuously because of changes in processes, IT infrastructure or other changes. For assessments that are based on questionnaires this is an intricate task, since it must be identified on which questions changes have an effect. In the presented approach based on assessment patterns, a connected graph structure of the former status is already present. This result of the last assessment can be used as a base line along with the actual version of the pattern pool on the mobile client for the update.

Based on this information, changes or extensions can be identified with the interview partners and described in the mobile client with reference to the last status. Also for the association of measurements to weaknesses in the backend, the former choices can be used as a reference.

6.5 Discussion of the Approach

The approach of a pattern based assessment in the area of compliance with legal regulations with a focus on SMEs is promising after the assessments performed so far. The tool-set is used by the data protection officials of the project partners. They perform assessments of external organisations with the help of the tool-set presented here already since several months. Based on assessments that need to be performed, the pattern pool is created on demand. At the moment most patterns that are needed in typical SME assessments are already modelled in the pattern pool. But mainly patterns for Business to Business (B2B) scenarios were created. Therefore the consideration of the rights of the data subject, as needed in Business to Customer (B2C) scenarios, is not modelled until now to the full extent.

To keep the concept of patterns simple, the case that potentially a measurement can lead to additional weaknesses is not modelled in the tool-set. Hints concerning these situations documented in the description of patterns. When such a situation occurs, the weakness has to be added to the assessment result.

7 Conclusion

The proposed concept of patterns for assessment is already used in a prototype of the described tool-set for assessments at SMEs, by a project partner. There also the current pattern pool was developed based on the experience of data protection officials. In the future, the pattern concept, which seems very promising,

has to be evaluated further. Beside that, the concept of analysis graphs has to be investigated after an appropriate amount of assessments is performed.

It is an interesting question to what extent the concept of patterns for assessment can be generalised to other fields or larger organisations. There a corporate pattern pool might be needed to model the specifics of the organisation. The question there is to what extent the benefits that are present in the case of SMEs as transparency and a common thread in interviews can be kept while the effort for the modelling of patterns is still reasonable.

Acknowledgement: This work was supported by the Federal Ministry for Economic Affairs and Energy through the Central Innovation Programme for SMEs (ZIM) (grants KF3081801KM2, KF2842903KM2).

References

1. Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design patterns: elements of reusable object-oriented software*. Pearson Education, 1994.
2. W.M.P. van der Aalst, A.H.M. ter Hofstede, B. Kiepuszewski, and A.P. Barros. Workflow patterns. *Distributed and Parallel Databases*, 14(1):5–51, 2003.
3. Dirk Riehle and Heinz Züllighoven. Understanding and using patterns in software development. *TAPOS*, 2(1):3–13, 1996.
4. Matthias Rodeck, Caroline Voigt, Arndt Schnütgen, Ina Schiering, and René Decker. Toolgestützte Assessments zu Datenschutz und Datensicherheit in kleinen und mittelständischen Unternehmen,. In *GI-Jahrestagung*, pages 575–586, 2014.
5. Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814). `http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html`.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML`.
7. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). `http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN`.
8. Johann Bizer. Sieben Goldene Regeln des Datenschutzes. *Datenschutz und Datensicherheit-DuD*, 31(5):350–356, 2007.
9. Federal Office for Information Security (BSI). BSI-Standards 100-1 100-2 100-3 100-4, 2008. `http://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html`.
10. Michael Gruber. Isis12 - Informationssicherheit für mittelständische Unternehmen. In *D-A-C-H Security 2013, Nürnberg*, pages 275 – 282. syssec, 2013.
11. Thorsten Humberg, Christian Wessel, Daniel Poggenpohl, Sven Wenzel, Thomas Ruhroth, and Jan Jürjens. Ontology-based analysis of compliance and regulatory requirements of business processes. In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science (Closer 2013)*, pages 553–561. SciTePress, 2013.

12. Siv Hilde Houmb, Folker Den Braber, M Soldal Lund, and Ketil Stølen. Towards a UML profile for model-based risk assessment. In *Critical systems development with UML-Proceedings of the UML02 workshop*, pages 79–91, 2002.
13. Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. *Model-driven risk analysis: the CORAS approach*. Springer, 2010.
14. Christopher Alexander, Sara Ishikawa, and Murray Silverstein. A pattern language: Towns, buildings, construction (center for environmental structure series). 1977.
15. Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, Michael Stal, Peter Sommerlad, and Michael Stal. Pattern-oriented software architecture, volume 1: A system of patterns, 1996.
16. Marco Brambilla, Piero Fraternali, and Carmen Vaca. BPMN and design patterns for engineering social BPM solutions. In *Business Process Management Workshops*, pages 219–230. Springer, 2012.
17. Munawar Hafiz. A pattern language for developing privacy enhancing technologies. *Software: Practice and Experience*, 43(7):769–787, 2013.
18. Munawar Hafiz, Paul Adamczyk, and Ralph E Johnson. Growing a pattern language (for security). In *Proceedings of the ACM international symposium on New ideas, new paradigms, and reflections on programming and software*, pages 139–158. ACM, 2012.
19. Jaap-Henk Hoepman. Privacy design strategies. In *ICT Systems Security and Privacy Protection*, pages 446–459. Springer, 2014.
20. Nick Doty and Mohit Gupta. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.385.6907`.
21. Business Process Model and Notation (BPMN). Version 2.0. *Object Management Group specification*, 2011.