# Privacy in the Life-Cycle of IT Services – An Investigation of Process Reference Models

Saskia Viktoria Rother, Ina Schiering

# Privacy in the Life-Cycle of IT Services - An Investigation of Process Reference Models

Saskia Viktoria Rother[1] and Ina Schiering[2]

[1] sas.rother@ostfalia.de
[2] i.schiering@ostfalia.de

**Abstract.** During the whole life-cycle of IT services privacy as expressed by user requirements and data protection legislation should be respected. There are several existing assessments for the assurance of privacy requirements in IT services. Other approaches like privacy protection goals allow already the integration in the design of a service. However, unlike information security, privacy is not incorporated in the best practice process reference models that are used to manage the life-cycle of IT services. In this paper widely-used process reference models CMMI and ITIL are analysed. It is investigated for these reference models to what extent privacy is already incorporated and what existing approaches could be recommended otherwise.

**Keywords:** life-cycle of IT services, privacy, process reference models, CMMI, ITIL

## 1 Introduction

Complex IT services often in the form of public cloud services are a vital part of our lives and an increasing amount of personal data is processed in these services. The internet is a main source of information, social networks allow interaction and communication, smart phones with a variety of apps accompany the daily life of people. The next step are devices like e.g. smart watches and monitoring devices e.g. for monitoring sport and other activities. But despite the fact that there is a data protection legislation in Europe since the 90s also today it is not anything but granted that privacy is respected. Concerning smart phone apps see the Opinion 02/2013 on apps on smart devices of the Article 29 Working Party [1]. Additionally, violations of privacy do not only happen during the realisation of a service but often during the operation or evolution of services.

In the European Union the legal framework for the processing of personal data consists of the European Data Protection Directive 95/46/EC [2], the e-Privacy Directive [3] with amendments Directive 2006/24/EC concerning data retention and Directive 2009/136/EC. Since January 2012 there exists a draft of a general data protection regulation [4] which is currently discussed. An interesting aspect of this draft is for example the incorporation of Privacy by Design.

But how to ensure that the regulatory framework is respected during the development, operation and termination of the IT service?

In this paper we investigate the approach of integrating privacy requirements in the life-cycle of IT services by incorporating them in process reference models, which describe best practices for the different phases of the service life-cycle.

The connection between data protection regulations and frameworks for information security is investigated in Meints [5]. Here we widen the scope to reference models for the whole life-cycle of IT services. Today process reference models are widely used in organisations: In a recent review of 23 studies about the use of ITIL for IT service management of the APMG, it was mentioned [6, p. 6] that between 28% and 77% of the organisations incorporated in the studies adopted ITIL. As a reference model for development processes CMMI is frequently used according to a survey concerning governance in IT [7, p. 26]. Therefore an overview is given for CMMI, ITIL, and TOGAF, COBIT which are also widely used. CMMI and ITIL are investigated in detail.

In Section 2 we present the process reference models we consider and investigate to which extent privacy requirements are considered and which existing concepts would be appropriate in the context. Afterwards in Section 3 we analyse where links to privacy are already incorporated in the reference models and classify the existing links. After this analysis we investigate in Section 4 which methods to design and control data privacy are available and discuss in Section 5 where these approaches are applicable in the reference models and in the service life-cycle in general.

## 2 Process-Reference Models in the Service Life-Cycle

The life-cycle of an IT service starts with requirements analysis, incorporates the design and implementation of software, the architecture of the system and the service operation. A typical model to represent these releases is the V-Model. It is a model for system development considering all phases of the development process as requirements, design, implementation, test and maintenance. The form of the "V" suggests that the development of tests is already started after the requirements are specified. During the operation phase continuously new releases of the service are realised and released until the service is terminated.

Therefore in all of these phases the privacy requirements have to be ensured. For each part of the life-cycle there exists process reference models that are widely used and considered as a best practice. Process reference models describe a set of processes and outcomes of processes that are relevant for the designated area.

For the design and implementation of an IT service we consider CMMI [8]. Concerning the development of architectures TOGAF [9] is investigated and as a best practice reference model for IT service management ITIL [10] is considered. As a model for the governance of the service life-cycle we incorporate COBIT [11] in this analysis. The focus of this paper is on CMMI and ITIL.

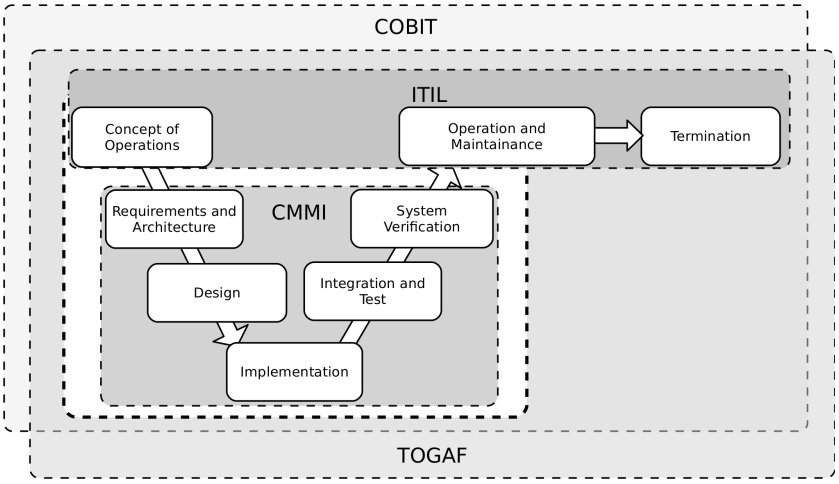


**Fig. 1.** Reference models and V-model

### 2.1 CMMI for development

The Capability Maturity Model Integration (CMMI) for development [8] is developed by the SEI (Software Engineering Institute at Carnegie Mellon University). The aim of this process framework is auditing and process improvement for development processes. The focus there is on organisational processes.

In CMMI practices needed in the development phase are grouped into process areas, (e.g. requirements development (RD), supplier agreement management (SAM), project planning (PP), technical solution (TS), validation (VAL) and verification (VER)). For each process area goals, practices and outcomes of these practices are described to allow for an appraisal (audit) of the development process of the organisation. Based on this process framework the maturity or capability of the development processes of an organisation is investigated. Capability Levels state to what extent the goals and practices in a certain process area are realised. To reach a Maturity Level, a defined set of process areas has to be established within the organisation to a designated level. These levels are initial, managed, defined, quantitatively managed, optimised and are described via generic and specific goals and practices. Therefore CMMI for Development can be used via Capability Levels for the individual improvement of process areas in an organisation whereas Maturity Levels allow for a benchmarking of the whole development process.

### 2.2 ITIL

The Information Technology Infrastructure Library (ITIL) [10] which is now available in the version ITIL 2011 is a best practise framework for IT service management (ITSM). The focus is on service orientation in information technology which allows for an alignment of IT services with business processes. ITIL is

a description of processes, roles and tasks that are needed to provide IT services. There the whole life-cycle of an IT Service is supported with the phases service strategy, service design, service operation and continual service improvement. ITIL can be used as a process framework for an ISO/IEC 20000 certification, the International Service Management Standard for IT service management. Since the focus of ITIL is on the management of IT Services but does not address software development or IT architectures, it could be used in addition to methodologies for these areas.

### 2.3 TOGAF

The Open Group Architecture Framework (TOGAF) [9] is developed by the Open Group. The framework is focussed on the development of an enterprise architecture. This architecture consists of the domains business, data, application, technology which describe the structure of an enterprise. Besides designing, planning and implementing, such an architecture, the framework provides also assistance for migration planning and governance.

### 2.4 COBIT

COBIT 5 (Control Objectives for Information and Related Technology) [11] is developed by the ISACA. It is a best-practise framework focussed on governance and management of enterprise IT. COBIT is based on so-called key principles, e.g. meeting stakeholder needs, enabling a holistic approach, separating governance from management. Beside the key principles COBIT is focussed on the notion of enablers. Examples of enabler dimensions are principles, policies and frameworks, processes, organisational structures.

COBIT has an overlap with TOGAF and ITIL, but is not intended to replace these frameworks. The aim of COBIT is to describe requirements concerning these processes unlike ITIL and TOGAF where best practices for processes are described.

### 2.5 Categorisation of Reference Models

To investigate the consideration of privacy in reference models and recommend existing concepts concerning privacy to fill in gaps, a categorisation of reference models is proposed. First the models can be distinguished concerning the level of detail in which processes are described. There are the possibilities that processes are defined in the form of best or good practices or on the other hand that only requirements for processes are stated.

Reference models like ITIL and TOGAF contain descriptions of abstract best practice processes that can be used as blueprints to define processes for IT service management (ITIL) resp. the development of an enterprise architecture (TOGAF). The focus of reference models like CMMI and COBIT is to describe merely requirements for processes and other elements needed concerning the

models. But there is no guidance for the implementation of the processes. The aim of these reference models is to allow for audits in organisations. This is in particular an element of CMMI where maturity levels are an important aspect of the models.

The other dimension which is investigated here for a categorisation of reference models is the intended audience of the reference model. Reference models can address the technical level or the management level of an organisation. None of the reference models investigated here address the basic technical level of software development or IT operation in detail, i.e. how a backup of a system is realised in IT operation or which rules for static analysis and metrics are used in the development phase of a software project. The reference models addressing the technical level contain processes for the management of development or IT operation. This focus on the management of technical processes can be perceived in ITIL and CMMI. The other models, TOGAF which is focussed on enterprise architectures and COBIT where the aim is the alignment of IT with business goals, have a management perspective.

The focus of this paper is on CMMI and ITIL. Hence reference models with a focus on the technical level are addressed. But these two models already cover all phases mentioned in the V-model (see Figure 1) and the two general approaches of reference models are addressed, i.e. best practice processes and describing requirements for processes. It would be interesting to widen the investigation on frameworks addressing the management level. There TOGAF and COBIT are important frameworks to consider according to [7].

## 3 Existing Links to Privacy

In the context of these reference models and considerations concerning categorisation, the existing references to privacy are investigated. Here we distinguish the following possibilities how privacy requirements can be integrated.

The strongest form of mentioning privacy is to address directly privacy requirements in the mandatory part of the reference model. Additionally, there are often recommendations concerning privacy in the reference models where requirements to privacy are mentioned or documents are described with a focus on privacy. But these are only recommendations which are not mandatory. Often legal requirements are mentioned in general. This encompasses privacy requirements based on legal regulations. Beside these explicit links to privacy we consider implicit links, e.g. when privacy requirements are defined in the requirements definition phase, as an implication they are tested during the validation and testing phase.

### 3.1 CMMI

In CMMI for development [8] privacy is not mentioned directly in a mandatory way, but there are references to legal requirements in general and for these legal requirements and their implementation examples with a relation to privacy are

mentioned. For a better understanding of the references to privacy the respective process areas are described first.

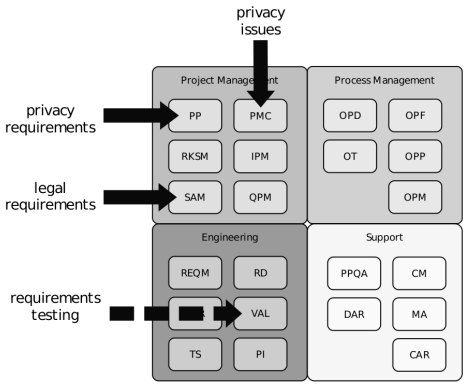


**Fig. 2.** CMMI and links to privacy

In the following the investigation of the process area project planning (PP) is detailed to illustrate the structure of process areas (see [8]). The aim of this process area is to establish and support project activities. It has 3 specific goals (SG), one of which is "SG2 Develop a Project Plan". There in the specific practice "SP 2.3 Plan Data Management" the management of all data during the project is mentioned which encompasses e.g. requirements, meeting minutes, or specifications. There are example work products for the specific practice mentioned. An example is a document about privacy requirements [8, page 292]. It is not a mandatory document, but an example of a work product. In subpractice 1 of SG 2.3 "Establish requirements and procedures to ensure privacy and the security of data" [8, page 293], privacy is stated.

The next reference can be identified in the process area "Supplier Agreement Management (SAM)". The purpose of this process area is the management of the purchase of products, The legal requirements are mentioned in the examples of the subpractice 6 from the specific practice "SP 2.1 Execute the Supplier Agreement". This subpractice states the management of reviews with the supplier. Review of the supplier's compliance with legal and regulatory requirements is listed as an example [8, page 371].

The process area "Project Monitoring and Control (PMC)" is responsible for measuring progress in the project. An important aspect concerning measuring project progress is the investigation of issues in the project. Privacy issues are named as an example for an issue: The specific goal "SG 2 Manage Corrective Action to Closure" has the sub practice "SP 2.1 Analyse Issues". There in subpractice 1, as an example for issues, privacy issues are mentioned [8, page 278].

Beside that, there are requirements in CMMI, which are often typical privacy requirements, but used in a different context. In the following we state an example: In the basic support process area "Measurement and Analysis (MA)" in the specific practice "SP 1.3 Specify Data Collection and Storage Procedures" there in subpractice 6, it is stated "Who is responsible for data storage, retrieval, and security?". Furthermore in "SP2.3 Store Data and Results" the aspect "Retention period for data stored" is stated. There in subpractice 4 privacy is mentioned "Prevent stored information from being used inappropriately." [8, page 188]. But here the focus is on the data needed during the project. Therefore this is not incorporated in the overview.

An implicit link to privacy is incorporated in the process area "Validation (VAL)". There the aim is the verification of requirements. Hence implicitly also the privacy requirements are tested.

### 3.2 ITIL

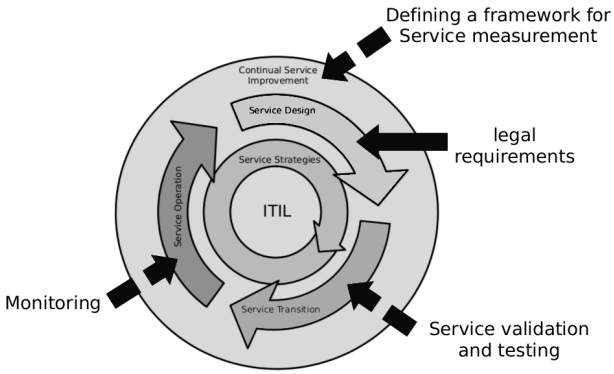


**Fig. 3.** ITIL and links to privacy

For the reference model ITIL there are mainly privacy requirements mentioned in the Service Design phase as an explicit statement. In the phase Service Design the data and information management is mentioned as technology-related activity. Concerning this activity it is described that legal requirements concerning privacy, security, confidentiality and integrity of data have to be considered. This data and information management can be incorporated in an Information Security Management System (ISMS) that is also mentioned in ITIL.

Implicitly in the phase Service Transition all requirements, hence also the privacy requirements are validated and tested. In the phase Service Operation the service is monitored which should also encompass the privacy requirements and in the Continual Service Improvement a framework for service measurement and improvement concerning the requirements is implemented.

## 4 Defining and Auditing Privacy Requirements

There are several approaches for incorporating privacy requirements. In the following, we give an overview of approaches for defining and auditing privacy requirements and describe in which part of the service life-cycle they can be applied.

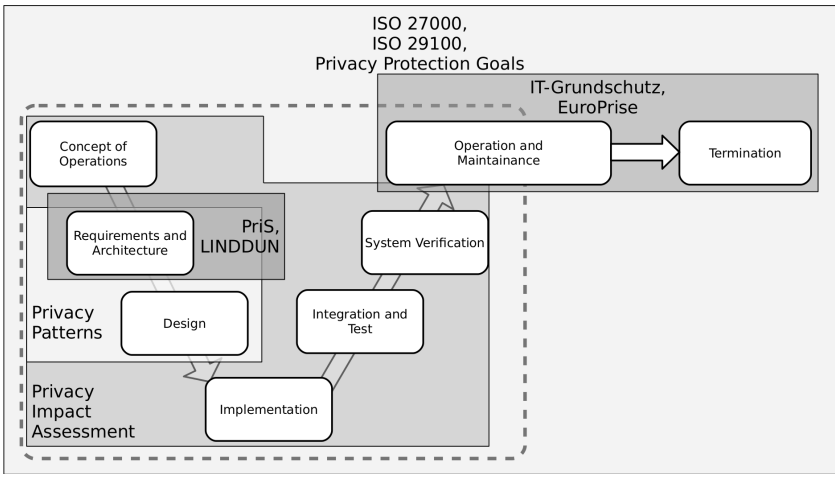


**Fig. 4.** Categorisation of reference models

The first type of approaches are assessments which are appropriate in the service operation phase of the service life-cycle. These audits are complex tasks, but can be applied to any service also without incorporation into process reference models.

Concerning auditing of European legislation like the data protection directive, assessments like EuroPriSe [12] can be used. Concerning a more general approach which is not focussed on European legislation in ISO 27000 [13] an Information Security Management System is defined. From a more technical point of view this can be investigated with the approach IT-Grundschutz [14], where aspects of privacy are integrated in a detailed security framework.

Beside that in ISO 29100 [15] a privacy framework is defined. In connection with this standard in ISO 29101 a privacy reference architecture is stated. With connection to the process assessment model of ISO 15504 [16] in the draft of ISO 29190 a privacy capability assessment model is proposed where also the maturity of the protection of personal data in an organisation will be addressed.

Instead of auditing a service during the service operation phase there exists also the approach of privacy impact assessments (PIA) [17] which are intended to be integrated in the risk management of the project. See [18] for an overview about PIAs resp. [19] for a detailed report about PIAs and different risk management methodologies. Hence PIAs are conducted already during the start of

the project and updated in the next phases and when there are changes in the project. Therefore a PIA is a possibility from the point of view of governance and management to incorporate privacy requirements in the service life-cycle.

Beside these examples of audits and assessments there exists approaches that are also applicable from a more technical point of view. One of these approaches are privacy-specific protection goals. These are based on the security protection goals Confidentiality, Integrity, Availability and are accompanied by goals focussing on privacy, i.e. Transparency, Intervenebility and Unchainability (see Zwingelberg et al. [20]). This approach is already incorporated in the LDSG of Schleswig-Holstein [21]. It can be used in requirements engineering to define the privacy requirements of potential users based on the legal obligations. These stated requirements can be used during the whole life-cycle.

There are also several approaches with a focus on requirements engineering. Here we mention Privacy Safeguard (PriS) [22], where privacy requirements are modelled as organisational goals and LINDDUN [23], which is based on data flow diagrams that are used to perform a thread analysis.

Other approaches also focussing on a technical point of view are based on patterns which are e.g. used in software engineering. The PrimeLife Policy Language [24] is a structured approach to the definition of user requirements concerning privacy. Beside that Doty and Gupta have developed the so called Privacy Patterns [25]. Privacy Patterns are example solutions for typical situations where personal data is used in services.

## 5 Gaps in the Existing Links to Privacy

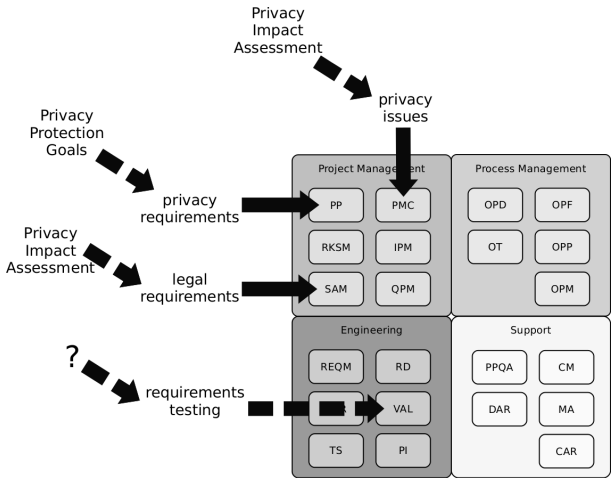


**Fig. 5.** Gaps concerning CMMI

How can the existing links to privacy be addressed with existing approaches concerning privacy?

In CMMI in the process area PP [1] privacy requirements should be stated. There in general privacy protection goals are an appropriate tool. Beside that when the service addresses end users, also approaches like the PrimeLife Policy Language can be used. The same argument applies to SAM where project data is addressed. Concerning PMC where during the project also privacy issues should be monitored and corrective actions applied and SAM which addresses the compliance of suppliers with legal requirements during the project especially risk management based approaches like PIAs are useful. Only for the implicit statement of privacy concerning the validation and testing VAL, there is no existing methodology that can be applied.

Concerning ITIL in the Service Design phase legal compliance of services is addressed. There also approaches as privacy protection goals for describing privacy requirements and PIA approaches to check these requirements during the project can be used. At the end of the development phase assessments like EuroPriSe can be used to check the compliance of the service with legal requirements concerning privacy. But there is a gap concerning testing of privacy requirements during the realisation phase of the project. There is no methodology to check privacy requirements as other requirements via tests that can be performed regularly during the project.

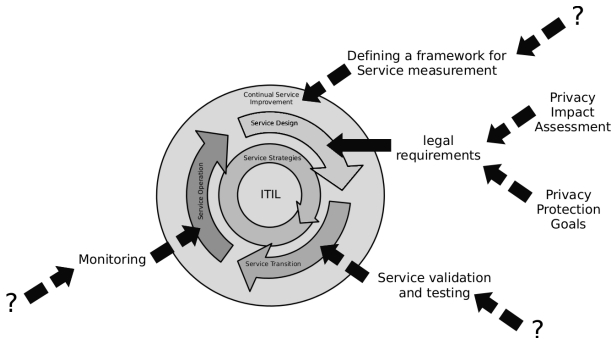


**Fig. 6.** Gaps concerning ITIL

To ensure that the privacy requirements are also preserved during the operation of a service, assessments can be updated resp. repeated periodically as it is addressed in ITIL in general by the Continual Service Improvement. But there exists no methodology to monitor privacy requirements between assessments e.g. after a change of the service. Since these assessments are quite complex this approach is not feasible. Also the implicit links to privacy concerning testing, monitoring and the definition of a framework for service measurement in

[1] see Section 2.1 concerning abbreviations

the form of key performance indicators (KPIs) are not addressed by existing methodologies.

## 6 Conclusion

During the service life-cycle of IT services there are already various references to privacy in the process reference models investigated here. In most of the cases, especially concerning requirements analysis and auditing there are existing approaches to integrate privacy in reference models.

But at the moment there exists no approach for testing of privacy requirements during the development phase of a service, for monitoring of these requirements during the operation phase of the service and for key performance indicators (KPI). These gaps will be investigated in future work.

Such methodologies could also be used to integrate privacy requirements in light-weight models as agile software development which are often used for the realisation of frequently changing services as cloud services and smart-phone apps.

## References


1. Article 29 Data Protection Working Party, WP 202 Opinion 02/2013 on apps on smart devices, European Commission, 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.
2. 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.
3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.
4. 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/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:HTML.
5. Martin Meints. The relationship between data protection legislation and information security related standards. In Vashek Matyas, Simone Fischer-Huebner, Daniel Cvrcek, and Petr Svenda, editors, *The Future of Identity in the Information Society*, volume 298 of *IFIP*, pages 254–267. Springer Berlin Heidelberg, 2009.
6. Rob England. Review of recent ITIL studies (APMG), 2011. http://www.best-management-practice.com/gempdf/Review_ITIL_Studies_White_Paper_Nov11.pdf.
7. IT Governance Institute. Global Status Report on the Governance of Enterprise IT (GEIT), 2011. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITGI-Global-Survey-Results.aspx.

8. CMMI Product Team. CMMI for Development, 2010. http://www.sei.cmu.edu/reports/10tr033.pdf.
9. The Open Group. TOGAF Version 9.1, 2011. http://pubs.opengroup.org/architecture/togaf9-doc/arch/.
10. Cabinet Office. ITIL V3, 2011. http://www.itil-officialsite.com.
11. IT Governance Institute. COBIT 5, 2012. http://www.itil-officialsite.com.
12. EuroPriSe (European Privacy Seal), 2008. http://www.european-privacy-seal.eu.
13. ISO/IEC. ISO/IEC 27000 - information technology security techniques information security management systems overview and vocabulary, 2009.
14. 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.
15. ISO/IEC. ISO/IEC 29100 - information technology – security techniques – privacy framework, 2011.
16. ISO/IEC. ISO/IEC 15504 - information technology process assessment parts 1-5, 2003-2012.
17. Information Commissioners Office. Privacy Impact Assessment Handbook, 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html.
18. David Wright and Paul De Hert. *Introduction to privacy impact assessment*. Springer, 2012.
19. David Wright, Kush Wadhwa, Monica Lagazio, Charles Raab, and Eric Charikane. Privacy impact assessment and risk management, Report for the Information Commissioners Office, May, 2013. http://www.ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf.
20. Harald Zwingelberg and Marit Hansen. Privacy protection goals and their implications for eid systems. In Jan Camenisch, Bruno Crispo, Simone Fischer-Hbner, Ronald Leenes, and Giovanni Russello, editors, *Privacy and Identity Management for Life*, volume 375 of *IFIP Advances in Information and Communication Technology*, pages 245–260. Springer Berlin Heidelberg, 2012.
21. Landesdatenschutzgesetz Schleswig-Holstein, 2012. http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=DSG+SH+%C2%A7+21&psml=bsshoprod.psml&max=true.
22. Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. Addressing privacy requirements in system design: the pris method. *Requirements Engineering*, 13(3):241–255, 2008.
23. Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, 16(1):3–32, 2011.
24. Gregory Neven Vimercati, Stefano Paraboschi, Eros Pedrini, Franz-Stefan Preiss, Dave Raggett, Pierangela Samarati, Slim Trabelsi, and Mario Verdicchio. Primelife policy language. 2009.
25. Nick Doty and Mohit Gupta. Privacy Patterns, 2012. http://privacypatterns.org/.