FIDIS

Future of Identity in the Information Society

Title:	"D14.8: Privacy in Business Processes"
Author:	WP14
Editors:	Prof. Dr. Günter Müller (ALU-FR) Maike Gilliot (ALU-FR)
Reviewers:	Thierry Nabeth (INSEAD) David-Olivier Jaquet-Chiffelle (VIP)
Identifier:	D14.8
Type:	[Deliverable]
Version:	0.9
Date:	Friday, 08 May 2009
Status:	[Final]
Class:	[Public]
File:	

Summary

This deliverable presents approaches for privacy in business processes where personal data is stored on the business partners' site, such as in applications for eHealth or loyalty programmes. It presents current approaches elaborated within FIDIS to privacy in business processes. The deliverable describes the threats to privacy in this setting and the underlying trust model. In addition to technical mechanism it also presents organisational means to preserve privacy.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Européen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	04.12.2008	• Initial release of (Maike Gilliot) • First version of Table of contents (Maike Gilliot)
0.2	29.01.2009	• Agreed on TOC with main contributors (Maike Gilliot) • Update Abstract
0.3	28.02.2009	• Integration of the contributions from Freiburg (Maike Gilliot, Rafael Accorsi), SIIRRX (Rani Husseiki), TU Dresden (Stefan Berthold) and ICCP (Martin Meints and Harald Zwingenberg)
0.4	31.3.2009	• Integration of the contribution form ICCS (Vassiliki Andronikou) and updated contribution from SIRRIX (Rani Husseiki)
0.5	20.04.2009	• Introduction, conclusion and executive summary (Maike Gilliot)
0.6	22.04.2009	• References (Maike Gilliot)
0.7	26.04.2009	• Release for internal review (Maike Gilliot)
0.8	06.05.2009	• Updated references and changes to the document as suggested by the internal reviewers
0.9	8.05.2009	• Layout and final corrections to the refernces. Final version

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Maike Gilliot (ALU-FR)
2 (Introduction)	Maike Gilliot (ALU-FR)
3 (Scenarios)	Vassiliki Andronikou (ICCS)
4 (Legal Requirements)	Harald Zwingenberg (ICCP)
5 (Privacy Threats)	Maike Gilliot (ALU-FR) Section 5.1; Rani Husseiki (SIRRIX), Section 5.2 ; Martin Meints (ICCP) Section 5.3
6 (Organisational approaches)	Martin Meints (ICCP)
7 (Technical approaches)	Stefan Berthold (TUD) Section 7.1; Sven Wohlgemuth (ALU-FR) Section 7.2; Rani Husseiki (SIRRIX) Section 7.3
8 (Conclusion)	Maike Gilliot (ALU-FR)

Table of Contents

1 Executive Summary

Note: This section is mandatory for all deliverable and should help to get an overview of the topics covered in the document.

Privacy for data providers and compliance for data consumers. Personal data is shared amongst business partners within intra- and inter-organisational business processes. The advantages of such services for the customer are uncontested, as are the user's privacy concerns: threats to privacy are a main hurdle for the acceptance of such services and processes on the user side (Sackmann, Strüker, 2005). Furthermore, the protection of privacy is an interest of service providers as well in order to meet the user's requirements (cf. the big-brother awards) and to comply with legal and contractual requirements.

As the deliverable tackles organisational and technical means to privacy in business processes, the **target audience** are mainly technical readers interested in technical organisational aspects of compliance and, especially privacy, in business processes. The first Sections (Section 2, 3 and Section 5) are the basis of the report. Starting from this basis, legal (Section 4), organisational (Section 6) and technical (Section 7) aspects and approaches are presented.

The **objective of this report** is to identify privacy threats in intra- and inter organisational business processes and to present technical and organisational means to control the dissemination and the usage of personal data, which is shared among business partners.

Approach of this report. Understanding privacy in information systems as the user's right of informational self-determination, privacy threats in business processes are identified. Recently publicly reported incidents of misuse of personal data on a large scale are analyzed. The analysis shows, that both technical shortcomings (no logging of data access for example) and organisational shortcomings (missing security level agreements in the case of outsourcing) allowed the incidence to happen. Based on those attacks, the legal requirements are analysed (Section 4). Security standards as organisational means to privacy are presented in Section 6. Further, a data protection management process is presented providing a general framework to control monitor and enforce on an organisational level data protection. The technical mechanisms in Section 7 present user centred mechanisms, namely the DREISAM protocol and DATA TRACK. Further, mechanism to control data usage on the providers side are presented: A mechanism for secure logging as a building block for any kind of a posteriori validation and Virtual Trusted Domains, setting up a trustworthy environment for process partners. At the end, we present a futuristic version of the scenario and the outlook section.

The **results of this report** is a comprehensive description of the threats related to personal data in business processes and approaches to control the usage of personal data in such settings. The mechanisms presented here haven been elaborated within the FIDIS project. Data protection is relevant for data providers and – for legal reasons – for data consumers as well.

2 Introduction

Recent advances in infrastructure technologies combined with the great standardisation efforts on processes, communication of information (messages exchanged) and data encoding are gradually enabling e-collaboration among participating entities across organisational borders.

Intra- and inter-organisational business processes between entities of a domain (such as depicted in the Scenario in Section 3) reduce costs among collaborating entities within the domain and are a basis for advanced services to citizens and customers. To achieve this, personal data, such as medical records, need to be shared and processed by a multitude of different entities for a multitude of different purposes.

To preserve the privacy of the data owner in such business processes requires organisational and technical mechanisms to ensure that the data owner can control the usage and the dissemination of data concerning him. The goal of this study on "Privacy in Business Processes" is to provide an overview of different approaches that have been developed within FIDIS Workpackage 14 to tackle the privacy problem in such settings.

2.1 Privacy for data providers and compliance for data consumers

In this context, privacy is not only about controlling what information is revealed to the communication partner, but also on how the communication partner further uses and processes this data.

The goal of privacy mechanisms for users is to control and limit the disclosure of personal data. However, in personalized services this approach is not any longer sufficient, as those applications *require* personal data. In consequence, users need mechanisms controlling how data is used *once it has been released* ("usage control") (Pretschner, Hilty, Basin, 2006). Figure 2.1 shows in an abstract way the parties involved and the data flow between those parties.

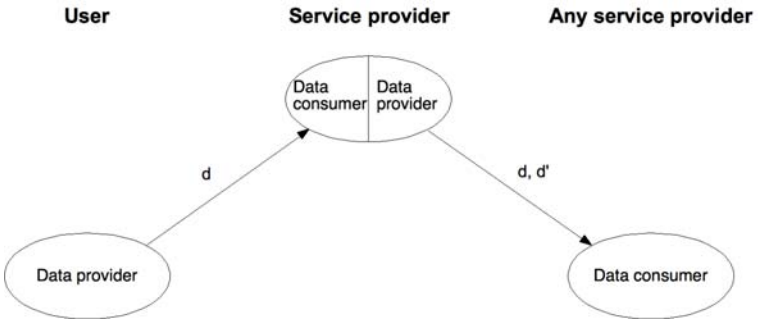

Figure 2.1: Usage control model (Pretschner, Hilty and Basin, 2006)

Access control is about controlling what data the data provider (or the data owner, e.g., the patient) releases to the data consumer (e.g., the doctor, hospital). The released data is modelled by the arrow marked *d*. Usage control is about how the data consumer processes and disseminates the data. The data consumer (e.g., a doctor) may change its role and becomes a data provider to some other data consumer (e.g., the insurance company).

As such, privacy is a major concern for users providing personal data. But, additionally, the usage of data is also a major concern for data consumers. Legal frameworks and contractual requirements (such as the organisations' privacy policy) have to be respected. In addition to the European Data Protection Directive 95/46/EC, domain specific regulations have to be respected. Compliance to such laws and standards is an ongoing effort for organisations.

Apart form legal consequences, privacy concerns of users privacy may also have a negative impact on business. For example, the retailer group Wal-Mart combined RFID-tagged articles with video surveillance, but stopped it after sharp criticism of privacy activists and users. The idea of the German retailer Metro Group to establish customer loyalty cards with embedded RFID tags allowing for RFID-based surveillance (Chicago Sun-Times, 2003), was dropped as well[4].

To sum up, each party involved in the business process wants to control the usage of personal data for its specific reason, according to the concept of multilateral security (Rannenberg, Pfitzmann, Müller, 1999).

2.2 Structure of the Report

The study tackles organisational and technical means to privacy in business processes. The first Sections (Section 2, 3 and Section 5) are the basis of the report describing the scenario, threats and reports on recent incidents with personal data. Starting from this basis, the legal requirements are analysed (Section 4). Security standards as organisational means to privacy are presented in Section 6. Further, a data protection management process is presented providing a general framework to control monitor and enforce on an organisational level data protection. The technical mechanisms in Section 7 present user centred mechanisms, namely the DREISAM protocol and DATA TRACK. Further, mechanism to control data usage on the providers side are presented, such as Virtual Trusted Domains for setting up a trustworthy environment for process partners. The report closes with an outlook- and summary section.

[4] Cf. http://www.bigbrotheraward.de

3 Example Scenario: eHealth

As an example for cooperation of different entities within a domain, we introduce an eHealth scenario as motivation. We present the collaborating entities within the broader health domain and depict – in a narrative way – how their collaboration provides advanced services to patients. To achieve this, personal data, such as medical records, needs to be shared and processed by a multitude of different entities for a multitude of different purposes. How advanced eHealth services may look like in the future, is presented in Section 3.2. Probably, even more personal data will be shared between the entities, which we will discuss further in the Conclusion in Section 8. Within the health domain, the main actors are:

- **Healthcare Provider:** private or public hospitals, clinics, private doctors. Roles within this entity include doctors, nurses, the billing section, the supply management section, among others.

- **Health Insurance Organisation:** a government-sponsored social insurance organisation or a private insurance company. The insured individual pays (directly themselves or through stoppages) premiums or taxes to the Health Insurance Organisation it has registered to in order to help avoid high or unexpected healthcare expenses. Health Insurance Organisations closely cooperate with the Healthcare Providers in order to proceed with transaction clearing of the healthcare-related expenses of the covered individual. Quite often this process does not only involve the communication of the receipts and the appropriate supporting documents but also a negotiation process between the two parties due to their conflicting interests, leading to slow cycles of information exchange.

- **Clinical Research Institution/Organisation:** a public or private entity performing clinical research (including clinical trials, animal testing etc)

- **National Drug Organisation:** an organisation responsible for protecting public health related to the circulation of drugs, medical related material and cosmetics among others by evaluating and approving new safe and efficient drugs.

- **Pharmacy:** it provides the prescribed medication to the patient and based on the Health Insurance Organisation the patient is registered to as well as the related policies requests for a specific percentage of the total amount of money or even the whole sum.

- **Statistical Company:** an entity responsible for collecting information based on specified surveys

3.1 Today

> *Mr Mark Peterson insured at Insurance Organisation X in Italy is travelling quite often in his country for business purposes. A few years ago he had an infarction and since then he is following a specific medication he must strictly adhere to. Although he has reduced his*

working hours following his doctor's advice for anxiety elimination in his daily life, he is still a dedicated financial consultant at his company in Napoli. After a long meeting at his enterprise headquarters in Rome he felt chest pain and intense discomfort and took his heart pills as indicated by his doctor in such cases. Nevertheless, his pain wouldn't ease and he decided to call his doctor who advised him to go immediately to the closest hospital (Hospital Y with which his Insurance Organisation X cooperates with) and get examined. At Hospital Y the doctor requests from Mark to provide information about his medical history, allergy list, medication list and past and current indications and he creates an Electronic Health Record (EHR) for Mark within the hospital. After making the appropriate exams, the doctor decides that Mark should be admitted in hospital for a couple of days so that his heart is monitored.

In the meanwhile the doctor updates the patient's EHR within the hospital with the new exams taken as well as the admission details, including admission time, hospital department, floor, room, supervising doctor. During Mark's staying at the hospital and after several exams made, the doctor decides that he should increase the dosage Mark's medication for a couple of days. After two days, Mark is ready to leave the hospital. The doctor prescribes him with new temporary supplementary medication and Mark goes to the billing department of the hospital. In the meanwhile, the doctor updates Mark's EHR with the medication administered. The hospital employee at the billing department requests a list of the exams that Mark took at the hospital, medication he was administered during his staying both followed by their cost and his insurance details from his Electronic Medical Record. The patient gets a receipt for these exams and pays 25% of the total cost based on his insurance organisation's policy and after he signs the receipt, he receives a copy and he leaves the hospital.

The hospital sends to the Insurance Organisation X a total report of the patients treated within it who are insured at X within the end of the week. The insurance organisation imports this report to their billing system and proceeds with the payment after checking the claims and their justification. In the meanwhile, Mark will be soon out of pills after the increase in his medication dosage and needs to follow the new medication the doctor prescribed him for a few days. Hence, he goes to a pharmacy the doctor suggested based on the list of cooperating pharmacies with his insurance organisation. The patient

pays 25% of the total cost of the pills, while the pharmacist submits the drug purchase at the online system which is interlinked with the insurance organizations. The insurance organisation receives the request through the system and is displayed with the medication the patient bought followed by the justification, the patient's details, the related billing information and the pharmacy's details. As Mark is

worried about his health status, he decides to visit his personal doctor in Napoli. For this reason, he calls him and arranges an appointment with him for the following day. The doctor's secretary updates the patient EHR in his hospital with the upcoming appointment.

3.2 In Future

Peter Smith is a security technologies consultant and has many customers across Greece. A few years ago he was diagnosed for myocardial infarction and since then he is following a specific medication he must strictly adhere to. During his business trip in Patras, he felt an intense chest pain and decided to go to the closest hospital. Peter visits the available doctor at the cardiology department, who accesses Peter's Electronic Health Record in order to view his medical history, his allergy list, his current medication as well as indications. After making some exams, the doctor decides that Peter should be admitted to the hospital for a couple of days for precautionary reasons. The doctor's secretary updates Peter's EHR with the hospital admission information and the exams results.

In the meanwhile, Dr Steven Morrison, a well-known clinical researcher, is designing a set of large-scale clinical trials for the investigation of the Thyroid Hormone replacement therapy on patients with myocardial infarction. During the clinical trial design phase and after setting this test of hypothesis as well as the inclusion and exclusion criteria and his preferences for the participation of patients in the clinical trials, Dr Morrison uses an advanced target selection system that automatically identifies patients eligible to participate in clinical trials by accessing and properly filtering based on the clinical trials specifications patients information in their EHRs. During this process, Peter seems to be included in the list of most suitable potential patients that could participate in the clinical trials. His contact doctor gets informed on this selection and is requested to communicate with Peter in order to let him know. As Peter is currently admitted to the hospital and given his quite tight schedule, he refuses to take part in the clinical trial. The contact doctor reports Peter's decision to Dr Morrison and the latter goes through the alternative choices in order to finalise his patient groups.

After Peter's close health status monitoring, the doctor decides that he should increase Peter's medication for a couple of days and subscribes him new temporary supplementary medication for a week. The new exams he took as well as the medication he was administered are included in his EHR. Peter is now ready to leave hospital. The hospital employee at the billing department requests from the EHR the list of the exams that he made at the hospital, the medication he was

> *administered during his staying as well as the admission details all followed by their cost and his insurance details. Peter signs the receipt gets a copy of it and leaves the hospital.*
>
> *At the Insurance Organisation X that Peter is insured to the clerk goes through a list of payment requests notifications. Through each notification the clerk is able to access the patients' EHR and view details about the related charges, including hospital admission information (hospital information, number of days), medication administered (drug, quantity, justification), exams made, sanitation material used followed by their costs and justification per patient. In the meanwhile, Statistics company W is conducting a survey regarding the current healthcare costs in Europe and retrieves in information from the EHRs anonymously in order to gather and analyse this data*

The futuristic scenario takes into account technological and standardisation trends and shows what an extended business process in eHealth can look like in a couple of years. The personal data is even more disseminated for different purposes. In order to make sure that the data owner will stay in control over her data, transparency enhancing mechanisms on the provider side and extended identity management tools on the data provider side will be necessary.

4 Legal requirements

The legal requirements of data handling in business processes are laid out in the national laws on data protection which are unified by the European Data Protection Directive 95/46/EC. The requirements set forth by these directives and the general principles of data protection that can be derived from the directives had been object of analysis in respect to business processes within FIDIS already (Müller, Wohlgemuth, 2007: 21–24).

4.1 Privacy in the European Data Protection Directive 95/46/EC

The Directive does not contain specific requirements for commercial transactions or business processes as such. The directive takes a rather broad approach, being universally applicable for any data handling by public institutions as well as private persons and companies. Some, but not all, member states differentiate in their data protection acts between public and private data processors, providing adapted rules for the private sector.[5]

The broad scope is laid down in Art. 7 of the Directive 95/46/EC, stipulating a ban for the processing of personal data, subject to the possibility of authorization. This means that any handling of personal data is generally forbidden except for cases allowed by law or an informed consent of the data subject. Due to its wide scope the directive and the national implementations can cover and solve issues raised by the majority of established and future business processes. However, the universal applicability is narrowed by exceptions to the scope of the directive and the permissions for data handling. Problems arise with borderline cases that may bear the potential to undermine the broad approach driven by developments which had not been foreseeable by the drafters of the directive in the 1990ies.

A clear, and in the field of business processes irrelevant, exception concerns matters of the police, judicial co-operation and criminal prosecution.[6] These issues fall out of the regulatory power of the European Community as they are part of the European Union's third pillar.

A historic exception from the directive concerns unstructured files which are manually processed. This exception is of inferior role as unstructured files are of no relevance in business practices today and only constitute a limited threat to privacy.

The definition of personal data may raise more issues in respect to the interpretation and application of the term "identifiable natural persons". Even though the Art. 29 Working Party already issued a working paper on this question[7] and a related decision of the European Court of Justice exists[8], the findings are regularly questioned by data processors. A recent case is the newly arisen debate about the character of dynamic IP-addresses as personal data in Germany.[9] Even if the clarification of the Working Party was widely accepted, that all "*the*

[5] E.g. the German Data Protection Act provides for such a diversification in sections 2 (§§ 12-26) for public entities and section 3 (§§ 27-38a) for other entities.
[6] See Art. 3 Sec. 2 of directive 95/64/EC.
[7] Working paper 136, available online: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
[8] Judgement of the Court of 6 November 2003, C-101/01 - Linqvist, available: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=601J0101&lg=en
[9] After the district court Munich decided in opposition to previous court rulings, and the opinion of the Art. 29 Working Party the specialized press took up on that debate again, leading to uncertainty within the relevant community.

means likely reasonably to be used by the controller or by any other person" to identify an individual must be taken into account it might merely shift the uncertainty. Data processors and subjects will then need to explore what means and external data reasonably may be used to identify a person and to which extent possible future developments need to be considered.

4.2 Issues and limitations of current legal directives

The directive excludes data "handling by a natural person in the course of a purely personal or household activity" from its scope.[10] The extended use of automated data processing also within family internal and personal communication may pose new challenges in the application of the directive. The widespread utilisation of interconnected automated data processing bears the risk of loss of control by intended or unintended distribution of personal data. However, this question is not relevant for business processes and will not be further pursued within this deliverable.

The directive's scope is limited further in respect to information once manifestly made public by the data subject.[11] Due to indefinite retention periods of some web archives, the extended access possibilities of search engines' data mining technologies and the negligible price of data storage this will affect the data subject's right of oblivion. Here a need for action can be identified for European and national legislatives. Businesses may be affected by the desirable implementation of deletion periods for their processes which should be implemented even if personal information may be processed and stored freely at the time of collection and recording.

4.3 Outlook

Future developments will pose new challenges for privacy compliant business processes. Current technological and social developments such as grid and cloud computing already raise problem in respect to control over the data. Who is responsible for the personal data processed if a processor cannot be distinctly identified? Who will perform the data subjects' right of access if control is surrendered to unnamed third parties? How can an informed consent of data subjects be ensured in ambient intelligence environments where their data may be collected by unknown simple gadgets in the vicinity?

Some of these questions may be answered by sticking to the general principles of data protection as described in FIDIS Deliverable D14.2, others may require legislative actions or innovative technological solutions. In respect to profiling and Ambient Intelligence these challenges and possible solutions were already analysed in FIDIS Deliverables (e.g. Hildebrandt, Meints, 2006: 80–83; Gasson, Warwick, 2007: 10–12).

[10] Art. 3 sec. 2 second indent of directive 95/46/EC.
[11] See Art. 8 Sec. 2 (e) of directive 95/64/EC.

5 Privacy Threats: Experimental Study and Recent Cases

5.1 Threats overview

A classification of threats on the basis of the possible damages was made in 1960 by William Prosser (Prosser, 1960) and 2006 by Daniel J. Solove (Solove, 2006a). Solove "extends" the work of Prosser and takes the technical development on data processing and network connections since 1960 into account (Solove, 2006a). Based on his classification of the potentially damage-producing activities, the threats related to

- data collection (1),
- data processing (2),
- data storage (3),
- delegation (4), and
- Intrusion (5).

Figure 5.1 shows a business process and the potentially damage-producing activities.

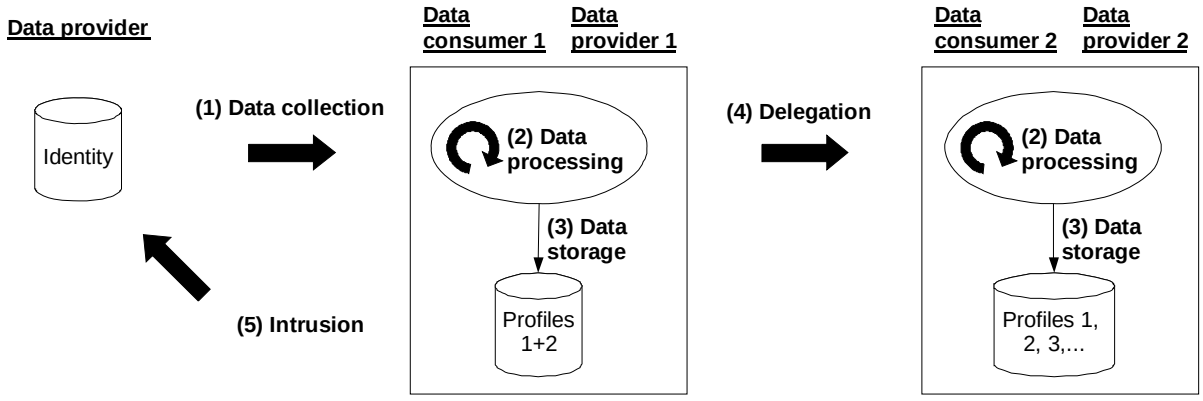

Figure 5.1 Activities with relation to the personal data of a customer[12]

5.1.1 Threats related to Data Collection

The users may be aware about the collection of their data, or the collection may happen unconsciously to the users. In the case of a conscious collection of data, a service provider requests personal data of a customer, such as delivery address or credit payment details. The data is collected for example via a web form. Thus, the users can decide whether to release their data to a given service for a specific purpose.

Critical to privacy is the unaware collection of data: Surveillance through video cameras in shops (Ball et al., 2006), collection of the IP addresses (Zugenmaier, 2003; Müller, Wohlgemuth, 2005) and the readout of RFID-tags (Strüker, Sackmann, 2004; Langheinrich, 2005) are examples of unconscious data collection, leading to severe privacy threats. In this

[12] Cf. FIDIS Deliverable D14.2: "Study on Privacy by Identity Management"

case, neither the service collecting the data nor the purpose nor the consent of the users are given.

Especially critical is the collection of identifying data, as it facilitates profiling and surveillance. Examples of identifying data are personal identity card number, social security number, a (vector of a) fingerprint, or the MAC address of a user's end device. Whereas MAC addresses or the number of the mobile phone can easily change over time, biometric identifiers and social security number identify users for their lifetime and are thus, especially carefully to be handled.

5.1.2 Threats related to Data Processing

A main threat to a customer's privacy in business processes is the use of collected data for purposes *other* than intended, for example, the aggregation of data from different sources and any kind of analysis on this data, such as profiling. Service providers can derive additional interests, behaviour and habits, creditworthiness and, for mobile customers, the user's movement profiles (Müller, Wohlgemuth, 2005). An advantage of such a profile formation could be the personalized product recommendations based on "similar" users. *Recommender systems*, as used in many online shops such as amazon.com, reduce the search effort (Lam, Frankowksi, Riedl, 2006).

However, such profiles can become disadvantageous, if users appear not to be trustworthy. This can lead to the desired service being declined or offered on poorer terms (Eifert, 2004). Moreover, the data used to profile the customer may be inaccurate or out of date, thus leading to a wrong assessment (Solove, 2006b; Hildebrandt, 2008).

A user-centred technical mechanism to control the disclosure of personal data is Data Track, as presented in Section 7.1.

5.1.3 Threats related to the Storage of Personal Data

Storage of personal data presents a threat to his privacy if the data storage temporally or quantitatively exceeds the customer's consent. If the purpose of the data collection is fulfilled, e.g. the service provider has delivered the service, the transaction has ended. Formally, the customer's consent for data processing also ends with the end of the transactions. Of course, legal requirements for data storage have to respected as well.

However, the European Data Privacy Directive 95/46/EG, as German Federal Data Protection Act and the "census judgment" of the Federal Constitutional Court explicitly allows exceptions if the general interest predominantly necessitates this. This applies, amongst others, in the case of state prosecution (European Commission, 1995). In Germany, for example, communication providers must store communication details to trace, in case of suspicion, illegal activities.

5.1.4 Threats related to the Delegation of Personal Data

In the scenario of business processes, personal data is disclosed by a service provider acting as proxy to further service providers. Data dissemination is a threat to privacy if the proxy can either disclose data to other service providers as those specified by the user or release more personal data to a service provider than specified by the user. The linking of profiles and identification of the customer can, among others, be negative consequences. Section 6.2 will show in more detail why (and how) the delegation of data has to be controlled in business processes.

The European Privacy Policy stipulates the notification of the person concerned with the first-time transmission of his data (European Commission, 1995). The German Teleservices Data Protection Act (TDDSG) allows the transmission of customer data for the purpose of market research which must however be anonymous (German Federal Government, 1997).

5.1.5 Threats by Intrusion

Intrusion into the business process can happen on all activities within the process related to personal data. For example, data can be intercepted by attackers during data collection. Intruders may spy out the content of the communication and modify the communication (delete messages, alter content of messages, replay messages). Especially messages delegating access rights can be misused by a malicious intruder. How right delegation based on identity management can be done in a secure way, is presented in Section 7.2. Passive observers are also a threat to privacy as they may create profiles based on the communication partners.

Intruders may also gain access to stored personal data. Generally, it is assumed that users store their data either on personal end devices or externally under control of a trusted third party, controlling access to the personal data. But faulty software or viruses or Trojan horses, can lead to unwanted disclosure of personal data. This threat will not be covered by the organisational and technical mechanisms presented within this study. Especially the technical mechanism are assumed to work correctly. The domain of security engineering studies how to design and to develop secure systems (Anderson, 2001).

To mention are further malicious staff members as attackers trying to gain access to the organisation's stored data. Beside a rigid access control mechanisms, a reliable log protocol is necessary to trace the activities performed on the data sets in order to detect misuse.

To sum up, intruders cause a multitude of very diverse threats. To tackle all those threats, goes far beyond the scope of this deliverable, so that the remaining of this deliverable focuses on the threats (1) to (4).

5.2 Study on Privacy violations

The extent of privacy violation by organizations collecting "Personally Identifiable Information" can hardly be estimated unless the evaluation of privacy breaches is done with respect to a privacy policy which is previously defined and agreed on between the organization collecting the information and its customers. Therefore, in order to assess and hopefully limit the extent of privacy violations in organizations the following should be addressed:

1) Pre-evaluation of the reliability of an organization's privacy policy, for example, by studying and evaluating the procedural and technical measures which are supported by the organization in order to enforce the privacy policy within its business processes.
2) Post-evaluation of the reliability of and the compliance with the privacy policy, for example, by evaluating and assessing the privacy breaches that occur – whether intentionally or unintentionally – with respect to the terms of the privacy policy.

While the first aspect is important and reflects a proactive approach towards establishing an organisational strategy for ensuring privacy in business processes (cf. chapter 4), the second aspect helps the organization figure out the weak points in the procedural and technical

measures applied. On the other hand, the customers are able to assess and judge on the compliance of the organization to the privacy policy.

For example, a study (CIPPIC, 2006a) on privacy violations in organizations has been carried on in 2006 by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) on 64 online retailers in order to assess their compliance with privacy laws. The results showed that a "surprising number" of companies failed to comply with the rules. The following is a summary of the aspects behind ineffective compliance to privacy laws by organizations:

- Difficulty of consumers to get answers regarding data protection policies of the company. Parts of privacy policies are unclear.
- Policies are often incomplete (unclear agreements with TTP).
- Notices of secondary usage of private data are often not included in the policy.
- No choice given to the customer to decide on unnecessary usage or disclosure of his data.
- Policy terms on sharing private data only with customer's consent are often disregarded.

Another study (CIPPIC, 2006b) y CIPPIC entitled "the Data Trail: How Detailed Information About You Gets Into The Hands Of Organizations With Whom You Have No Relationship" shows how customer private data is gathered and traded in the marketplace by organizations collecting information from customers. The study suggests that many organizations consider the benefits of sharing private customer data to outweigh costs. For example, private customer information is often traded between data owners and users. The study showed that mostly, consumer data is sold as lists of names and credentials, including telephone numbers, email addresses, and postal addresses. Sources of consumer data were found to be various retailers and service providers such as magazines, newspapers, email and other subscription services, travel agencies, product manufacturers (via registration/warranty cards), online educational and information services, and payment processing companies.

5.2.1 FIDIS Experiment

The FIDIS deliverable on an "Experimental Study on Profiling in Business Process" addresses this particular privacy violation trend in organizations. The study aims at collecting substantial proofs to trace the behaviour of commercial entities with respect to their handling of personal data. Basically, the experiments try to uncover the fact that personal data is passed through to other companies without the consent of the corresponding customers.

The methodology of the study fits with the 2nd option mentioned above, which is a form of post-evaluation of the compliance of organizations to privacy policies by means of experimental analysis. Personal data is marked (e.g., by slightly modifying names, data etc.) and given away to commercial companies (e.g., buying portals, club cards etc.) with the purpose of tracing the leakage of personal customer information based on, e.g., advertisements.

Categories

In order to make the range of target companies as wide as possible, we defined a set of categories of companies. The general categories were:

- "Basic life services" which included telephone, electricity, insurance, life insurance, banks, mobile companies and internet providers.
- "Online shops": clothes, books, auction systems, food, logistics, furniture, cosmetics, flight operators, email, lottery, pay-TV, newspapers, magazines.
- "Miscellaneous": catalogue sending, job search engines, social networking websites.
- "Bonus programs": gas stations points, flight operator miles, shopping cards, etc...

Company Category	Targeted	Company Category	Targeted
Electricity	2	Auction systems	2
Health insurance	3	Food stores	2
Mobile companies	2	Cosmetics stores	4
Internet providers	2	Flight operators	2
Catalogue	2	Email websites	3
Job search engines	4	Newspapers	4
Social networking	2	Magazines	2
Clothing stores	3	Bonus programs	5
Book stores	2		

Table 5.1: Categories

Variation scheme

We followed a straight-forward scheme for watermarking identities based on the idea to produce several identities from a real one. This was done by introducing slight variations that could also appear as data errors, namely variations in the spelling of non-western names, by permuting vowel letters in the first name and family name. Based on a systematic approach for permutations, we could obtain around fifty *derived identities*.

Procedure

A relatively long, non-western full name (first and last name) was chosen, and variations have been introduced in a way that is limited enough to appear as a spelling mistake (a typo) rather than an intentional variation or spelling of a different name. The original name was printed on the post box of the company, and a set of personal data (address of the company, email address, birth date, etc…) attributed to the name was created to form a full identity.

Fifty derived identities were created by introducing variations to the name, but leaving the identity attributes common to all names. Then, registration has been performed in each of the fifty chosen institutions, each with a distinct derived identity. So each derived identity is handed over to only a single business. The mapping between the derived ID and the Institution it has been sent to has been stored for correlation between received post or email and the sending institution on a later stage.

Results

A sample of the results that were received is provided below. For each received post or email, the category of the original company is noted (e.g. online shop, bonus program), as well as the existence of a prior privacy policy agreement with the customer, and whether this policy has been respected or not. The decision on whether a profiling trace is found is based on the fact that the post or email has been received from a company that has not been provided any identity information.

Result	**Result Category**	**Result Type**	**Company Category**	**Policy Agreement w/ customer**	**Policy Compliance**	**Profiling Trace**
Newsletter	Company Advertisement	Email	Bonus Program	Yes	Yes	No
Newsletter	Company Advertisement	Email	Online Shop	Yes	Yes	No
Promotion	Company Advertisement	Email	Online Shop	No	N/A	No
Newsletter	Company Advertisement	Email	Bonus Program	Yes	Yes	No
New Services Advertisement	Company Advertisement	Email	Online Bookshop	Yes	Yes	No
Newsletter	Company Advertisement	Email	Bonus Program	Yes	Yes	No
Discounts Advertisement	Company Advertisement	Post	Clothing Shop	No	N/A	No
Order Magazine	Company Advertisement	Post	Outfits Shop	No	N/A	No
Promotions	Company Advertisement	Email	Online Outfits Shop	No	N/A	No
Promotions	Other Company Advertisement	Email	Online Electronics Shop	No	N/A	Yes
Promotions	Company Advertisement	Email	Social Networking	Yes	No	No
Promotions	Other Company Advertisement	Post	Newspaper	No	N/A	Yes
Promotions	Company Advertisement	Post	Cosmetics	No	N/A	No

Table 5.2.: Overview of Results

A quick analysis of the results led to the following observation: the type of email/post received can be categorized into four cases:

a) A privacy policy on identity information usage is proposed by the company at the registration time, and the customer has supposedly agreed on, which makes the advertisements received by the company legitimate.

b) A privacy policy on identity information usage is proposed by the company at the registration time, and the customer has supposedly agreed on, but the advertisements received do not comply with the policy, which means that the company has misused the identity information without actually leaking it.

c) No privacy policy on identity information is proposed by the company at a first place, which makes "compliance to privacy policy" not applicable. However, the origin of the received item is the company itself, which means that the identity information has not been leaked.

d) No privacy policy on identity information is proposed by the company at a first place, which makes "compliance to privacy policy" not applicable. However, the item did not originate from the corresponding company, but from another company to which the identity information has been obviously leaked. This case is counted as a profiling case.

Further information on the experiment, results, and analysis are provided in the corresponding deliverable (D14.5).

5.3 Cases of recent privacy violations

In 2008 a number of privacy violations occurred in the private sector which were widely covered by the media and recognised by the general public in Germany and had quite some impact on the ongoing debate how to modernise the German Federal Data Protection Act (BDSG). In this section two selected cases will be presented, together with an analysis covering information security and data protection. These cases are

1. Loss of control about personal data in call centres and lottery companies, discovered in 2008
2. Loss of control about personal data at the German telecommunication provider T-Mobile in 2006

5.3.1 Case One – Call Centres and Lottery Companies

The first case became widely known in August 2008, when a CD with 17.000 addresses and bank accounts data were anonymously handed over to the Consumer Protection Centre Schleswig-Holstein (Verbraucherzentrale Schleswig-Holstein, VZ SH).[13] A few days later, mid of August 2008, two additional CDs/DVDs were handed over to the vz sh and the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH), the responsible Data Protection Authority. These CDs/DVDs contained additional 130.000 and one million data sets of personal data, varying in content and quality.[14] At the same time the

[13] See http://www.verbraucherzentrale-sh.de/UNIQ122405616029315/link481821A.html
[14] See https://www.datenschutzzentrum.de/presse/20080818-datenhandel-callcenter.htm

Federal Association of Consumer Protection Centres (Verbraucherzentrale Bundesverband) commissioned a private detective to buy as many address data from the illegal market as possible for 850 €. The detective returned with six million data sets within 44 hours.[15] So within a few days the loss of control concerning personal data affected millions of German citizen.

Before these cases of loss of control became known citizens complained at Consumer Protection Centres that money was debited directly from their bank account without contractual grounds. In many cases elderly people were concerned by this debit fraud, and the debits in many cases were related to lottery services[13] . Debit fraud uses the fact that banks in Germany in case of debits up to 100 € generally do not check the contractual grounds for the debit. Account holders can cancel a debit within six weeks quite easily, but need to check and evaluate money transfers regularly to be able to do so. In some cases the bank customers still may have a claim against their bank for reimbursement for the illegally charged amount. But enforcement of this claim may becomes more difficult and resource consuming.

The data sets from the CDs were analysed by ULD SH. This resulted in the following findings:[14, 16]

- The data sets on the CDs were prepared to be used for debit fraud. Selections were made covering elderly people (years of birth from 1930 to 1940), which maps with the complaints at Consumer Protection Centres already mentioned.
- In many cases the data on the CDs contained information concerning its origin.
    - As data "provider" a number of small and medium sized call centres could be uncovered, partially from meta data in excel files.
    - Data source and originally data controller in the sense of the European Data Protection Directive 95/46/EC were in many cases in Germany well known lottery companies and service providers (e.g. Norddeutsche Klassenlotterie (NKL), Süddeutsche Klassenlotterie (SKL), and lottery resellers (Lotto Team and the telecommunication provider Deutsche Telekom)).
    - In some cases data were collected in online lottery games.
- The analysis gave evidence that personal data regularly were bought, sold and exchanged.

The enterprises involved in the data losses reacted in a similar way, calling themselves victims of criminal manipulations.[17] In one case it became known how control about personal data got lost. In this case a call centre acting as service provider had unrestricted access to the customer relationship management system (CRMS) of the data controller. This included export functions. In addition the IT infrastructure at the call centre was not secured. Official and private USB devices could be attached to the computers allowing to easily copy and disseminate data.[17]

---

[15] See http://www.vzbv.de/go/presse/1045/

[16] See https://www.datenschutzzentrum.de/vortraege/20081201-meints-issec-datendiebstahl.pdf, especially slides 16 to 21

[17] For exaple the Deutsche Telekom, siehe http://www.heise.de/newsticker/Skandal-um-illegalen-Datenhandel-Auch-Telekom-Kunden-betroffen--/meldung/114444

5.3.2 Case two: T-Mobile

The second case already happened in 2006, but was taken up by the press again in 2008 at the beginning of October.[18] Already in 2006 attacker got access to the CRMS of T-Mobile, taking copies of 17 million data sets of customers. This became known because an eroticism service provider to whom the data sets were offered informed T-Mobile already in 2006. The responsible state attorney started investigations, but until 2008 nothing substantially happened.[19] T-Mobile started an investigation directed at copies of these data in the Internet. When the T-Mobile investigators were not able to find any data they concluded that no more copies were publically accessible, and the incident handling was obviously closed without taking care that the data of the eroticism service provider was deleted. This service provider kind of reopened the case by publically asking what to do with this data.[18]

When state attorney and T-Mobile reinvestigated the data source could be found. In this case the CRMS of T-Mobile was accessible via the Internet, and the access was protected insufficiently obviously using group accounts (e.g. for all employees of one T-Mobile shop) and weak passwords. T-Mobile account information already was well known by hackers.[20] Mid of October 2008 access control was improved by introducing a transaction number (TAN).[20] End of October 2008 personal consequences were taken by putting two employees on leave and structures were changed by introducing a new director for data protection.

5.3.3 Analysis

In the first case (call centres and lottery companies) loss of control in the majority of cases happened at external service providers (outsourcing partners) due to insufficient technical and organisational security measures. This includes:

- Insufficient access control for customer's data in call centres (at least for outbound activities access can be restricted to a list of customers per time frame). Responsible are data controllers (e.g. lottery company, Deutsche Telekom) and service providers (e.g. call centres).
- Lack of deactivation of software functionality not needed for the service. In one case the export of data from the CRMS of the data controller was not restricted. Responsible in this case are the data controllers.
- Lack of deactivation of interfaces (in this case USB) not needed in the call centres and lack of regulation how to deal with data media (in this case official and private USB sticks). Responsible in this case are the service providers (call centres).
- In addition organisational deficiencies can be observed in the context of outsourcing. In case security service level agreements were made correctly, implementation was not checked and enforced. Responsible in this case are the data controllers; this responsibility can not be outsourced and remains with the data controller. This is

[18] See http://www.heise.de/security/Alter-Raub-neuer-Skandal-17-Millionen-Telekom-Nummern-entwendet--/news/meldung/116913

[19] See http://www.heise.de/newsticker/Bericht-Erotik-Unternehmer-lagert-T-Mobile-Kundendatenbank--/meldung/117007

[20] Siehe http://www.heise.de/security/Spiegel-Telekom-Sicherheitsluecke-offenbart-30-Millionen-Handydaten-Update--/news/meldung/117229

explicitly stated in the Annex to Art. 9 BDSG, where data protection control in the context of outsourcing is defined as a control.

In addition it is worth thinking about the roles of the parties involved. Enterprises involved called themselves victims. From a legal point of view they were data controllers and data processors and thus responsible parties. The victims in these cases are the data subjects who suffered in some cases from significant financial losses.

In addition in these cases loss of control happened in the context of outsourcing. When planning outsourcing, branch specific aspects need to be taken into consideration. In Germany it is well known that especially small call centres suffer from cost pressure and pass this pressure on to their employees by paying small incomes.[21] Sometimes a very small basic income is paid, amended by additional salary in cases of success, e.g. in cases of concluded contracts. Typically for the definition of a "success" it does not play an important role whether a concluded contract is really fulfilled. The reason is based within the German Distance Contracts Act (Fernabsatzgesetz)[22] consumers may withdraw from contracts concluded via internet or phone without giving any reason within two weeks. This constellation fosters secondary use of personal data: Either selling the data, or, cross using data from one service customer in order to "optimising" the number of concluded contracts.

In the first investigated case the number of references to call centres in the illegally sold and transferred address and bank account data indicates structural problems in the area of information security and data protection in call centre sector. Such structural problems need be taken into consideration when outsourcing services in such a sector. Typically this leads to an increased investment into quality assurance, information security and data protection.

A change can also be observed for the assessment of data protection (or privacy) risk for data subjects. Outside the financial sector loss of personal data in rare cases lead to financial damage for data subjects in the past. This significantly has changed now, as far as data subjects were not able to reverse fraudulent debits within six weeks. Though no provable number of victims was reported so far, Consumer Protection Centres claim that this number is significant.[13]

In the second case also insufficient security measures, especially insufficient access control, enabled the loss of control over personal data.

In this case the management analysis is of interest. Though in 2006 neither the culprit nor the attack vector could be identified, the management came to the conclusion that no more copies of the data were available. At this point the security incident management was concluded without ensuring that known copies were deleted. The task of the security incident management at that point in time simply was not fulfilled.

Data protection experts for a long time indicate that the loss of control about personal data for the data subject potentially can be severe, as lost control cannot be reobtained easily if possible at all. For this reason the potential impact for the data subject can be long lasting or permanent. The second case indicates that this evaluation also may be true for data controllers, as a scandal caused by data loss may be "reanimated". In the context of risk

[21] See e.g. http://www.heise.de/newsticker/Gewerkschaft-fordert-Mindestlohn-fuer-Call-Center-Branche--/meldung/93871
[22] cf. Directive 1997/7/EC on the Protection of Consumers in respect of Distance Contracts.

assessment this means that an enterprise may face long lasting or permanent losses (annual loss expectancies, ALE) instead of single loss occurrences (SLO).

From a legal point of view in the cases described a number of laws were violated, but a thorough analysis exceeds the scope of this text. In the context of data protection violations concern especially the finality principle (§ 28 BDSG) and the security safeguards (§ 9 BDSG and the corresponding annex).

Conclusions and Recommendations

From a security point of view the conclusions and recommendations by far are not surprising, as they well map with technical and organisational security measures suggested e.g. in ISO/IEC 27002. Concretely the following aspects can be recommended:

- Implementation of the need-to-know-principle: Employees should get access only to data they need for official purposes. Access control measures need to be in place and effective. In case of outsourcing terminal services can be used, as they allow the implementation of access control measures by the data controller.
- Functionality of applications not needed (in this case export functions) should be deactivated. Data export can be avoided or at least hampered by using terminal services, as the access to data from export interfaces of the application can be refused.
- System interfaces not needed (in this case USB) should be deactivated. For this purpose commercial solutions are available on the market.
- The use of mobile data storage devices should be regulated and enforced.
- Access to applications and data should be logged; audit logs should be evaluated regularly.
- In case of outsourcing the conditions of the contract are important. In addition to service level agreements (SLAs) security service level agreements (SSLAs) need to be included, together with instruments to check whether these SSLAs are fulfilled (audits) and instruments to enforce them in case of deviations. In any case differences in economic (e.g. economic targets) and cultural aspects between data controller and outsourcing partner need to be taken into consideration. These differences can be significant e.g. in cases where the contract partner differ significantly in size and market position. In cases problems may arise from these differences, additional measures need to be agreed and implemented.
- In case a security incident occurs an effective security incident management and handling is important. In case of attacks special care should be taken to identify, block or at least hamper attack vectors and culprits. A security incident handling strategy focused on data copies likely will fail.

From a data protection point of view the following recommendation needs to be taken into consideration:

- The security incident management should check whether the risk assessment of data protection related risks still is up to date. In this context the conclusions from this analysis and planned changes in the context of the German Federal Data Protection Act (BDSG) need to be taken into consideration.

Possible Legal Consequences

Following the publication of the control losses concerning personal data a number of changes in the German Federal Data Protection Act were proposed and discussed. Some of them are quite far reaching, e.g. the suggestion made by the Senator of Justice of the Federal State of Hamburg in Germany, Mr. Steffen. He proposed among others to strengthen the civil law based claims of the data subjects.[23]

The status of the modernisation of the BDSG was summarised by Weichert (2008) and has not changed significantly since then. Based on a proposal by the German federal Government, a proposal for a BDSG-modernisation currently is discussed in both chambers of the German parliament. The proposal and the corresponding debate are concerning loss of control about personal data focused on the following issues:

- Strengthening of the informational self determination by reducing exceptions from the informed consent.
- Introduction of breach notifications in case of loss of control over personal data
- Transfer of the already existing prohibition of the coupling of a contract with the consent to process personal data for additional purposes from the Act on Telemedia (Telemediengesetz, TMG) to a general article in the BDSG
- Increasing of fines, introduction of so called "benefit absorption" in case of illegal economic transactions

However, these proposals are still controversially debated, as shown by the current reports from the Federal Council of Germany.[24]

[23] See http://www.hamburg.de/pressearchiv-fhh/1085860/2009-01-19-jb-datenschutz.html
[24] See e.g. Bundesratsdrucksache 4/09, TOP 24 from 13th of February 2009.

6 Organisational approaches to privacy in Business Processes

To realize security and privacy in organisations, technical mechanisms are not enough. The goal of best practices and of standards is to simplify the strategic planning, deployment and monitoring of security mechanisms. To this end, this section gives an overview of current standards for IT security and to what extend those standards help to enforce the legal privacy requirements as given in the European Data Protection Directive 95/46/EC (Section 6.1). The Data Protection Management Systems (DPMS) presented in Section 6.2 is meant to be an organisational framework for technical and organisational data protection measures within an organisation. Section 6.3 describes different criteria, such as the Process Maturity Model, to evaluate the quality of the Data Protection Management System.

Organisational issues include other very important issues, such as behavioural aspects (culture and change management, for example). However, those organisational aspects will not be tackled in this section and are out of scope of this deliverable.

6.1 Application of standards for security and IT Service Management

In the context of (information) security the European Data Protection Directive 95/46/EC[25] is not very specific. The Directive lines out security requirements, not concrete technical or organisation security measures. Relevant requirements extracted from the Directive are:

- Art. 17:
    - Protection of "personal data against accidental or unlawful **destruction or accidental loss**, **alteration, unauthorised disclosure or access** […] and against all other unlawful forms of processing"
    - Implementation of "appropriate **technical and organisational measures"**
    - An appropriate level of information security, (technical) **state-of-the-art**, **costs**, **data protection related risks** and the **nature of personal data** processed
- Art. 8 describes **special categories of personal data**: Data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health-related data, and data concerning the sex life of the data subject. It further points out that Member States shall generally forbid the processing of these data. Cases are described in which processing can be allowed and reference again is made to suitable safeguards in these cases.
- Recital 46 also points out many requirements also introduced in Art. 17. In addition the following aspects are introduced:
    - Technical and organisational security measures need to be applied in a way that they cover the **lifecycles of procedures**[26]**.** The "**time of design** of the

[25] Available via http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

processing system and […] the **time of the processing** itself" are explicitly mentioned as important phases to be covered to maintain security.

Reasons for the use of quite general requirements are among others (Meints, 2009, and references cited therein):

- Data protection legislation is developed in a different (mostly legal) domain compared to information security (mostly technical domain)
- Technology and as a consequence technical security measures undergo a rapid development and require frequent updates which is not desirable in the context of legislation

As a consequence and in the context of information security, the Directive also does not directly refer to standards. Other standards e.g. in the context of quality management and IT service management are also not referred to.

The following figure gives an overview on relevant standards referring to information security in organisations (mainly management orientation) and products (mainly technical orientation):

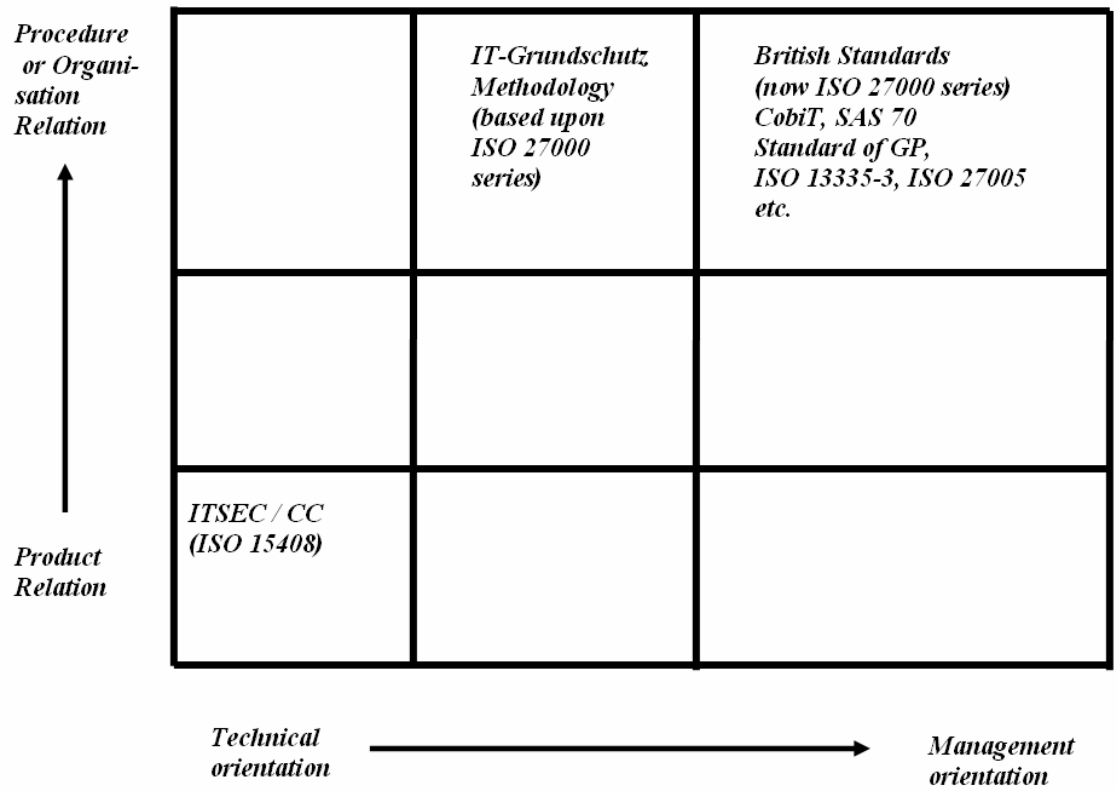

Figure 6.1: Categorisation of information security related standards[27]

[26] In this context a procedure is understood as a governmental or business procedure, covering one or more processes and relating Information and Communication Technology (ICT).
[27] Figure taken from (Meints 2009); this figure is based upon (Initiative D21 2001)

The most important standards introduced in Figure were already introduced in (Buitelaar, Meints, van Alsenoy, 2008: 30–33) and described in an overview by Meints (Meints, 2009a). A relevant question is how these standards relate to state-of-the-art in (information) security and thus how they can be used to fulfil the corresponding requirements in Art. 17 of the Directive. This question is important, as the content of these standards and their application differs in the targets. Some standards are a catalogue of good practices which can be used as a reference. Other standards are certification standards with certificates aiming at business excellence or best practice. Requirements in these standards may be very specific and exceed state-of-the-art. A classification towards the fulfilment or the exceeding of state-of-the-art by applying relevant standards in the context of information security was proposed by Meints (2009), as presented in Table 6.1.

In the context of IT operations and IT service management the IT Infrastructure Library (ITIL)[28] and the "Control Objectives for Information and related Technology" (CobiT)[29] are most relevant. Both already were briefly described in (Buitelaar, Meints, van Alsenoy, 2008: 29–30).

ITIL provides a framework of good-practice processes that can be use to fulfil organisational security requirements.

CobiT provides a set of control objectives and controls (structured lists of requirements) that help to fulfil technical and organisational security measures directly. CobiT also integrates compliance requirements and thus connects to - from the point of view of the applying organisation - relevant legislation.

[28]British Office for Government Commerce (OGC), *ITIL*, currently in version 3.0, available at <http://www.ogc.gov.uk/guidance_itil.asp>, last consulted 15 October 2008. Parts of ITIL version 2.0 are also internationally standardised as ISO/IEC 20000.

[29] US American Information Systems and Audit Control Association (ISACA), *CobiT 4.1*, available at <http://www.isaca.org>, last consulted 15 October 2008.

Standard	Content and remarks	State-of-the-art in security	Exceeds state-of-the-art in security
ISO/IEC 27001	Information Security Management Systems (ISMS)	X (partial implementation, especially concerning hierarchy and processes of the ISMS)	X (certificates)
ISO/IEC 27002	Code of Practice, catalogue of generic information security measures	X	
ISO/IEC 27005	Information Security Risk Management	X (risk assessment methods also can be applied in the context of data protection risks and the Privacy Impact Assessment (PIA))	
ISO/IEC 27006	Accreditiation Requirements; covering certificates for auditors and requirements for Certification Bodies (CBs)		X (certificates)
ISO/IEC TR 13335-3	Risk Assessment Methodology; withdrawn in June 2008	X (see ISO/IEC 27005)	
IT-Grundschutz Methodology	Three BSI-Standards and the IT-Grundschutz Catalogues	X (ISMS, risk assessment methodology and security measures in the Catalogues)	X (certificates)
CobiT V4.1	IT governance framework	X	
ISO/IEC 15408	Security certificates and protection profiles for ICT products	X (security functions)	X (certificates)

Tab. 6.1: Overview of the standards analysed[30]

[30] Table taken from (Meints 2009)

6.2 Data Protection Management Systems (DPMS)

Data Protection Management Systems (DPMS) are no official term introduced by the European data protection legislation. So far this term was introduced and used only on a national level.[31]

Based on the similar term "Information Security Management Systems (ISMS)" as defined in ISO/IEC 27001 DPMS can be understood as the organisational framework for technical and organisational data protection measures within an organisation. A DPMS contains at least the following components (Buitelaar, Kindt, 2009):

- Function bearer(s) that are qualified, able to enforce a privacy policy within the organisation, and able and willing to carry out their role not in conflict with other roles that are assigned to them; typically this function bearer is the called "Data Protection Officer (DPO)".
- A process framework (see e.g. Müller, Wohlgemuth, 2007).
- Documentation, among them the data protection policy, a data protection / security concept and operative documentation (e.g. an inventory of procedures, a process handbook, operational advice for employees, guidelines, documentation of the implementation of technical and organisational (security) measures, data protection and security management reports).

Important is the data protection concept. The data protection concepts describes for one or more business or governmental procedures

- Related ICT infrastructure, including applications, ICT systems, networking components and connections and physical and environmental infrastructure
- An assessments of data protection related risks in correlation with the data protection policy
- A risk treatment plan including technical and organisational measures; these measures also need to include tasks required by the legislator, for example the fulfilment of data subjects rights of information, rectification and deletion of personal data.

A good practice process model for the maintenance of a data protection concept including related supporting processes was proposed in (Müller, Wohlgemuth, 2007: 42–47). Meanwhile this process model was integrated into the data protection module[32] of the IT-Grundschutz-Catalogues, a collection of good practice security measures based on ISO/IEC 27002 provided by the German Federal Office for Information Security (BSI).[33] In the context of this integration the tasks in the processes were described more detailed (Meints, 2007). Since 2007 the data protection module is supported by all Data Protection Authorities in Germany (Simon, 2007). Currently a translation of this module from German into English is in preparation (February 2009).

---

[31] For example in Germany: Art. 8 of the decree of the Federal State of Schleswig-Holstein referring to the implementation of the data protection audit (Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG), https://www.datenschutzzentrum.de/material/recht/audit.htm

[32] See http://www.bsi.de/gshb/baustein-datenschutz/index.htm; the process model was integrated as measure M7.1.

[33] See http://www.bsi.de/gshb/index.htm

6.3 Improvement of effectiveness and efficiency of DPMS

As DPMS heavily rely on processes, generic measure to evaluate the quality of processes concerning as well effectiveness as efficiency also can be applied in this context. One possibility to evaluate processes qualitatively is the use of the Process Maturity Model (PMM, see e.g. Meints, 2007a; Buitelaar, Meints, van Alsenoy, 2008: 31). Depending on the version used, the PMM allows the evaluation of the maturity of processes in five or six levels (see Figure 6.1 for the five-level maturity model):

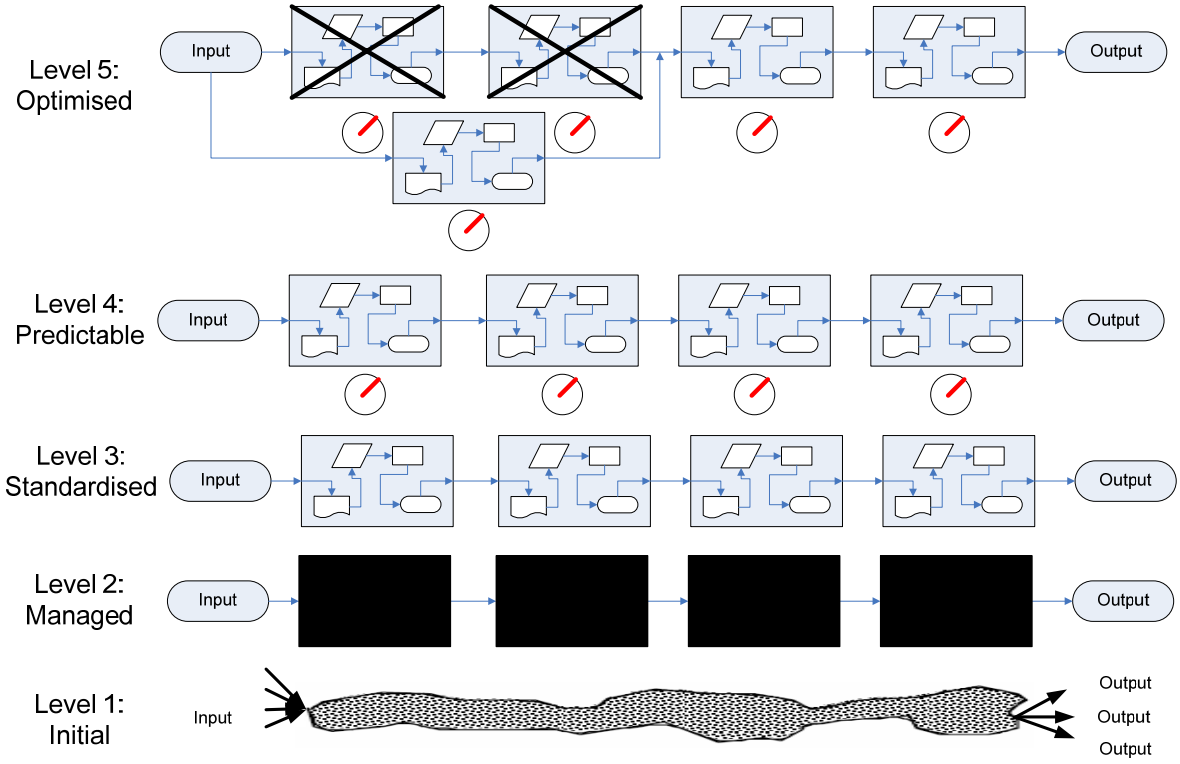

Figure 6.1: Levels of the Process Maturity Model (PMM)[34]

Based on the results of the evaluation a targeted improvement is possible, taking care first of all of the measures allowing reaching the next level of maturity.

An important aspect of the improvement of a DPMS is its integration in other processes with similar workflows and targets. Relevant neighbouring processes are the ISMS and the framework used for IT service management or IT governance as they likely include similar processes, usable structures and know-how. Though process integration does not lead to savings of complete disciplines and related tasks, resources required for process, task and infrastructure management can be reduced sometimes significantly.

One important example for possible benefits taken from process integration can be shown when viewing the planning phase for an application supporting a business process (see e.g. Meints, 2009b). Similar process tasks carried out by various function bearers with a different focus can be found for example in the management of requirements for the new application, testing and formal releasing. Stakeholders in these tasks may be (a) the specialist department

[34] Figure taken from (Buitelaar, Meints, van Alsenoy 2008: 31)

(functional requirements), (b) the IT department (integration into the IT infrastructure and IT service management), (c) the information security management (security requirements) and (d) the data protection management (data protection compliance).

In the context of information security the potential synergies are very obvious. They mainly cover

- Direct fulfilment of security requirements referring to data protection (delegation of tasks from the data protection management to the information security management). This becomes very obvious when looking at the data protection relevancy of security measures listed in the Baseline Protection Catalogues which is elaborated in a cross reference table in the data protection module.[35] As a summary almost all security measures in the Baseline Protection Catalogues are also relevant from a data protection point of view.
    - Concrete examples in this context can be the maintenance of the inventory of assets, the security concept and the documentation concerning the implementation of security measures.
- Use of the processes of the ISMS for data protection specific tasks by integrating tasks and processes, as lined out in the example above.
    - Complete process integration for example is possible e.g. in the context of security incident management and business continuity management.
    - Task integration is possible e.g. for the development and implementation of an (data protection and information security) education plan

[35] See http://www.bsi.de/gshb/baustein-datenschutz/dokumente/b01005_hilfsmittel_tabelle.pdf. The relevancy of the security measures is evaluated by mapping them to the eight data protection controls in the Annex of Art. 9 BDSG.

Concerning ITILv2 the potential synergies can visualised a follows:

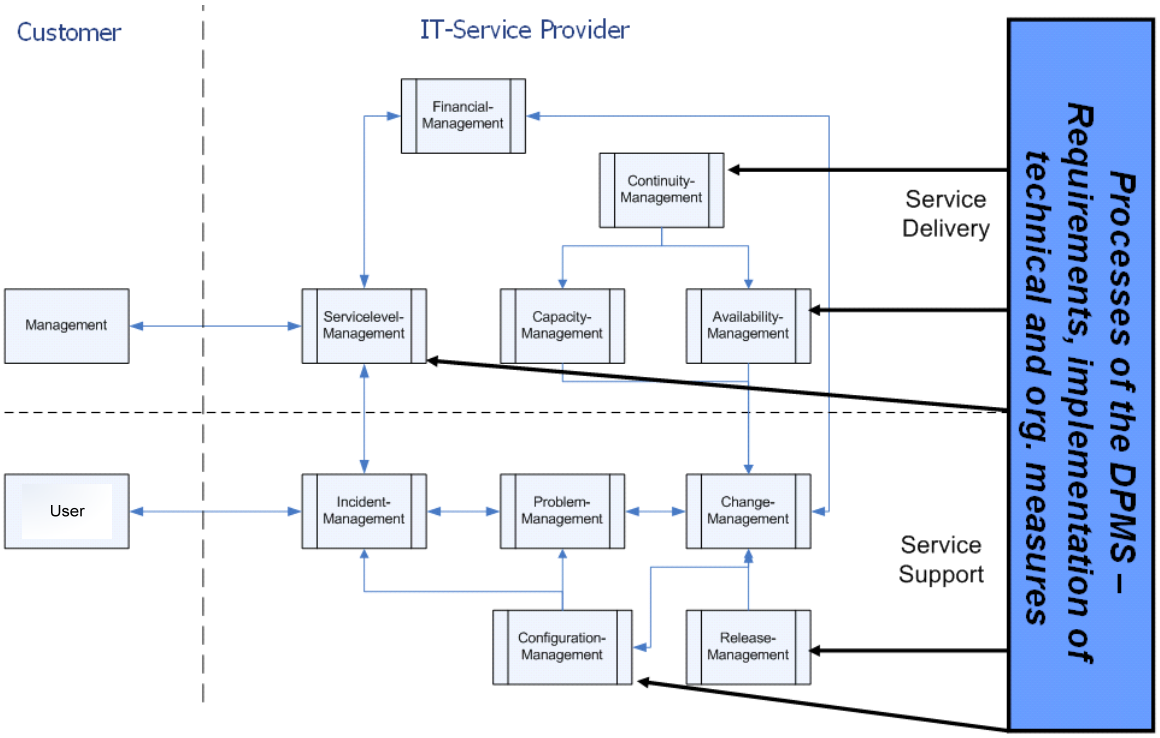

Figure 6.2: Potential synergies between ITILv2 and a DPMS

In concrete the synergies can be (Meints, 2005):

- Use of complete ITIL processes for data protection management purposes, e.g.:
  - Management of requirements, testing and formal releasing using release management.
- Use of ITIL process structures, know-how and resources for data protection management purposes, e.g.:
  - Business continuity management relying on the service continuity management.
  - Security incident management relying on incident and problem management.
  - Data protection service level agreements being managed in the context of the ITIL service level management.
- Use of infrastructure for data protection management purposes, e.g.:
  - The configuration management database (CMDB) for documentation and auditing purposes.

Why is the use of these synergies so important? Resources, especially for compliance, are limited in enterprises - they need to be used sparingly. In the long run only processes will be accepted that provide a relevant business contribution – which compliance of course can be – for a minimum of resources (efficiency). In addition, integrated and centralised processes are better accepted and implemented by members of an organisation. One centralised process can integrate all relevant stakeholders and will not be bypassed as easy as a number of parallel processes with similar target. From that point of view process integration also is important from the perspective of the effectiveness of the data protection management.

6.4 Conclusion

In the light of the recent privacy violations as analyzed in Section 5.3.4., the set up of organisational measures is at least as important as the deployment of secure mechanisms. The recommendations derived from the presented privacy attacks are technically easy to implement (such as more restrictive access control, limited functionality), but are challenging on the organisational level (controlled use of mobile data storage, efficient incident management). Organisational measures are complementary to technical mechanisms, attacking the privacy problem from different angels. The focus turns now towards technical mechanism.

7 Technical Solutions for Privacy in Business Processes

The design of secure and privacy preserving applications (either intra-organisational or inter-organisational) is the focus of the security engineering domain. Currently, security requirements are integrated by hand, which is difficult and error-prone and depends on the experience of the developer. Backes et al. (Backes, Pfitzmann, Waidner, 2003) present a framework to integrate security requirements in a formal and rigorous way during the software development phase. Another general approach is the Enterprise Privacy Architecture (EPA). It allows to identify business processes which make use of customers' personal data or attributes and to implement privacy regulations via privacy policies in an information system of a service provider (EPA is presented for example in D14.2).

The focus of this section is on mechanism (and not on general frameworks). All tool presented provide for users – to some extend – information and control on data usage. Data Track, presented in Section 7.1, is a user-centred tool to continuously keep track of the release of personal data to business partners. Dreisam, a set of protocols extending current identity management systems, is described in Section 7.2. It allows the user to control which business partners access their personal data, assuming the data provider to be trustworthy. The Trusted Virtual Domains in Section 7.3 allows to build up a secure and confidential environment for the processing of personal data.

7.1 Data Track

For achieving privacy in business processes, it is conceivable to have technical means in place at the site of the business partner that reliably control the flow of data and thus provide a source of trust for the customer. The alternative is that the customer has to keep track of what is happening and what is part of the deal herself. The data track is part of the latter kind of solution.

We have identified three main sources that describe requirements and solutions for data tracks. The first source (Brückner, Voss, 2005) describes a rather technical view on a data track which can be applied to web browser communication. The authors also maintain a reference implementation. The second source (Meints, 2006) describes the data track from a view legal view, i.e., it defines technical requirements and legal consequences of a yet non-existent data track solution. The third source (Pettersson, Bergmann, Fischer-Hübner, 2006) describes the data track with more detailed technical requirements. These are mainly outcomes of the PRIME project.

It can be conceived as the counterpart of customer relationship management (Brückner, Voss, 2005) or as a transparency tool which continuously keeps track of the release of personal data to business partners. In the best case, the data can be used as kind of evidence in disputes (Meints, 2006). Thus, an integral part of the data track is a database that contains all relevant records of communications with business partners for instant or later inspection. Usually, the vanilla database is accompanied with supplementary functionality, such as *searching* for instance all business partners that received a particular data item, *suggestion* of data sets with minimal privacy impact for future data releases, *simulating* the situation after planned but yet not performed data releases, or functionality for *exercising rights* granted by the EU Data Protection Directive 95/46/EC (Pettersson, Bergmann, Fischer-Hübner, 2006).

Data track provides transparency about *facts* that are processed by business partners, but not necessarily about the *consequences* of the data release (this corresponds to the top right cell in the taxonomy of transparency, as given in Table 1 in FIDIS Deliverable 7.12). It provides, however, transparency on the level of attribute *values* (right cells) and not only on the level of attributes alone. This makes the data track to a quite a powerful transparency tool, even though limited to the data which is available to the customer.

In a society where information is a good and privacy is traded against other values, the data track is also a kind of bookkeeping about the contracts that have been made. This makes it necessary that the data track is not only a log about released personal data, but also contains information about the legal circumstances in which the data has been released. Thus, the data track has to contain the basically information about

- the pseudonym which has been used by the customer to make the deal,
- personal data which has been disclosed as part of the deal,
- the recipient who received the personal data items,
- the date of transmission, and
- the privacy policy which is binding for both, the customer and the business partner. (Pettersson, Bergmann, Fischer-Hübner, 2006; Meints, 2006)

In addition to that basic information, there might be further relevant information that should be stored as well. For instance, *extra obligations* which are not part of the privacy policies can be of interest in later analysis or for reasons of evidence (Pettersson, Bergmann, Fischer-Hübner, 2006). Furthermore, the search in the data records might be facilitated by *tagging* and *commenting* (Pettersson, Bergmann, Fischer-Hübner, 2006) the records and thus enrich the plain records with semantics. This would also help with the interpretation of the rather technical form of records. Besides that, the data track can be complemented automatically by data from *supplementary information sources*. The availability of such information sources depends largely on the application area. If web services are involved, there might for instance be data about the business partner from the “whois” database, there might be references to different business partners that arise from linked content or advertisement on the web page of the primary business partner (clickstream graphs), there might be P3P policies in addition to privacy policies and business terms in different formats, and there might be data contained in cryptographic certificates that are applied in order to establish trustworthy and potentially confidential communication between the customer and the business partner (Brückner, Voss, 2005).

The data track is also an ideal starting point for the support of customers in exercising the rights granted by the EU Data Protection Directive 95/46/EC. The large amount of data gathered in the database of the data track can for instance be used to check whether the business partner acts in compliance with the policies and obligations that have been agreed upon. It is also well suited for suggesting and supporting the customer in requests for further data, rectification, or erasure of personal data at the site of business partners (Pettersson, Bergmann, Fischer-Hübner, 2006). This would even enable the customer to reverse data releases if possible.

At the same time, the data track may become problematic in terms of privacy (Meints, 2006). This is mainly the case, if such functionality is applied by professionals rather than private persons. In this case, the EU Data Protection Directive also applies to the data gathered in the

data track and is thus limiting the amount and the purpose of processing. Particularly, each business partner needs to be informed about the gathering of the data in the data track.

The ideas of providing a data track have been pursued in the PRIME project of the EU where the data track has been integrated in the larger setting of a privacy-enhancing identity management system (Hildebrandt, 2008), and by the PRIMA project at TU Darmstadt (Brückner, Voss, 2005) in which the data track has been integrated into an ordinary web browser. The focus of the PRIME project was on supporting the customer (or more generally the user of the identity management system) by metaphors in order to make her understand her current situation, her rights, particularly those of the EU Data Protection Directive, the effects of future data releases, and even support the customer by means of suggestions for future data releases or legal requests. Furthermore, PRIME was focused on checking and enforcing policies and obligations. The difference in the PRIMA project was that the researchers there assumed that the customer would understand the data stored in the data track as long as it is compiled in the right way and that the user would even know how to proceed in difficult situations. The research was mainly focused on developing a prototype that works fine in the scope of browsing the web. In this scope, the PRIMA project developed a set of quite sophisticated tools.

In summary, the data track is a tool for making privacy transparent. In general, it is limited to the data that can be gathered at the site of the customer, but in combination with the rights granted in the EU Data Protection Directive, it well suited for customers that intend to keep track and explore their current privacy situation.

7.2 The Delegation Problem

The unauthorized dissemination of personal data and the unauthorized delegation of access rights are major threats to privacy in business processes. Figure 7.1 illustrates the privacy problem using the example of loyalty cards in CRM.

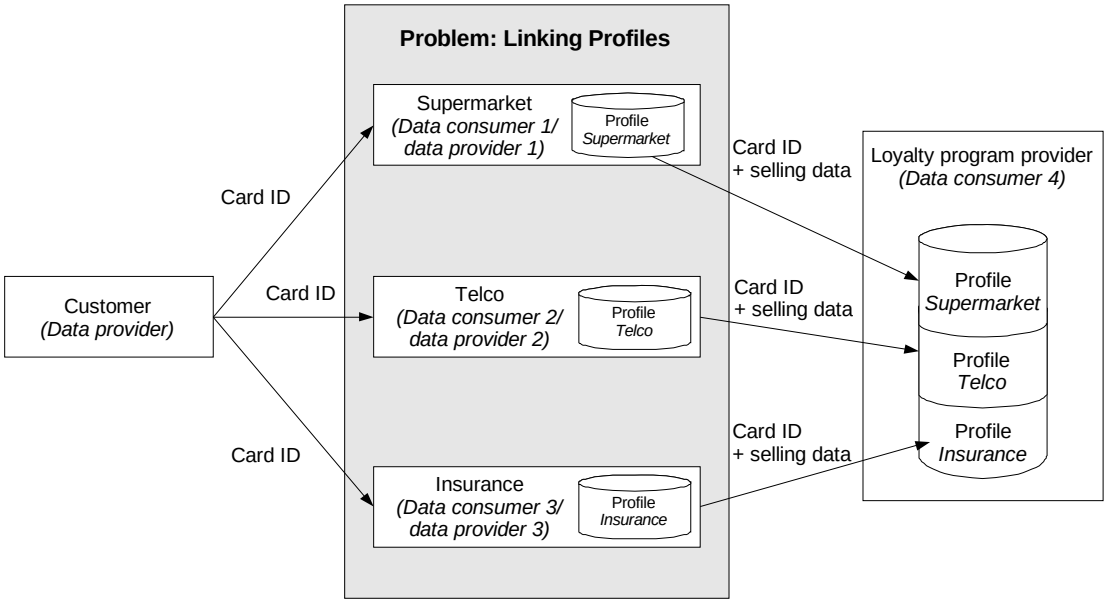

Figure 7.1 Linking customer's profiles by merchants when buying goods or services with a loyalty card.

Personalised services with several service providers require collection and delegation of personal data. The service providers collect personal data and delegate them to other service providers. Thus, a service may change its role: it may take the role of a data consumer or of a data provider. The challenge faced is whether the requirements of data protection legislation according to information self-determination can be fulfilled so that users are able to enforce the agreed rules for using personal data. An example of activities and role changes are customer loyalty programs (Customer Relationship Management – CRM).

7.2.1 Privacy Threat in CRM Systems

The case study CRM shows that, in practice, users have to trust service providers. They have to accept the general terms and conditions and thereby give service providers full authority to process their data. Technically, these rules regarding the collection and delegation of personal data correspond to provisions and obligations in order to get access on some personal data. The consent of a user is then commensurate with a delegation of a specific access right to this data in combination with the agreed rules. The evaluation of existing security tools for delegation of rights and for privacy shows their conceptional weaknesses: By delegating access rights, users are neither able to enforce the agreed rules nor to control the enforcement of delegated rights according to the agreed rules. They lose control of the access to their data. Consequently, the one-sided, practice-based trust model remains unchanged if these tools are applied.

The attacker can either be an intruder or the merchants themselves (cf. Section 5.1). Intrudes may want to violate the privacy of the users or disturb the merchant's systems. Merchants can attack the user's privacy by linking customers' transactions. This would allow to create a profile by virtually combining their single, merchant-dependent profiles. Merchants are able to link their profiles by the unique card number (*Card ID*) of customer's loyalty card. It follows that they know what this customer has bought at the supermarket, the pharmacy, and the insurance company.

Privacy as informational self-determination is violated, as the customer is not able to determine the disclosure of personal data. By linking profiles, customer's data are disclosed to other merchants and used for other purposes than those of the collection, since his profiles are now used by other merchants, too. Additionally, linking profiles is not an interest of the loyalty program provider. The collection of these profiles at his database empowers the loyalty program provider to analyze customers' profiles and to offer queries for marketing purposes. If the merchants are able to link their profiles without the loyalty program provider, the collection of profiles is worthless for the loyalty program provider. A merchant would not pose such a query at the loyalty program provider anymore.

Currently, the customer has two options for delegating an access right on his profile to a merchant:

- The customer issues a delegation credential for the merchant, e.g. a X.509 Proxy Certificate (Welch et al., 2004).
- A certifying authority (CA) issues a delegation credential for the merchant on behalf of the customer, e.g. a SPKI certificate (Ellison et al., 1999) or a Kerberos proxiable ticket granting ticket (Kohl, Neuman, 1993).

In both cases, transactions of a customer are linkable by every merchant and, in the second case, also by the CA. In the first case, the digital signature of the customer for his delegation

credential makes him traceable. In the second case, the identifier of a customer is fixed in a credential and obvious for every participating service provider. To solve this problem, we propose DREISAM, a set of protocols for the secure delegation of rights.

7.2.2 Secure Delegation of Rigths: DREISAM36

To close this gap and to realise the trust model where users need not trust service providers, DREISAM was developed. It is a set of protocols allowing to delegate securely access rights on personal data using credentials and extends the identity management system IManager (Wohlgemuth et al., 2004). During a protocol run no additional information about the user is published so that his transactions cannot be linked by service providers. We sketch the proof-of-concept implementation and an example from the CRM domain in order to show the interplay of the different protocols. A formal description of the protocols haven been presented in Deliverable D14.2 "Study on Privacy in Business Processes by Identity Management"(Müller, Wohlgemuth, 2007).

The proof-of-concept implementation considers an electronic bargain for a health insurer. It consists of five services, one CA and one user. The services are two health insurers, one pharmacy, one fitness centre and a loyalty service provider, as depicted in Figure 7.2. All service providers take part in the same loyalty program. It is assumed that services have already collected personal data of the user and forwarded to the loyalty program provider.

In order to offer a discount on a health insurance, the insurance provider wants to get access to a user's fitness centre profile (request for personal data by protocol A). The user agrees, but does not want the insurance company to access other personal data than the fitness center profile, e.g., his pharmacy profile. Therefore, the user delegates an access right via the CA to the insurance provider INSURE acting thereby with a transaction pseudonym (protocols B and C). The service of INSURE can now access the fitness centre profile (protocol D) on the loyalty provider's database.

However, the DREISAM system does not control how data is used once the request has been granted. In other words, the misuse or dissemination of data by INSURE cannot be prevented.

The proof-of-concept implementation of DREISAM is based on the identity management system iManager of the University of Freiburg (Wohlgemuth et al., 2004) and on the anonymous credential system IBM idemix (Camenisch, van Herreweghen, 2002). The iManager is extended by sub systems for data consumers, data providers, and for the CA. As presented in Figure 7.2., the DREISAM authentication service is responsible for requesting access rights and personal data (by running protocol A), and the DREISAM certification service issues Proxy Credentials and anonymous credentials (protocol B). The protocol D controls the access request of the data consumer.

[36] DREISAM is the name of the river crossing the city of Freiburg. Its little cascades remember the flow of the steps in a protocol.

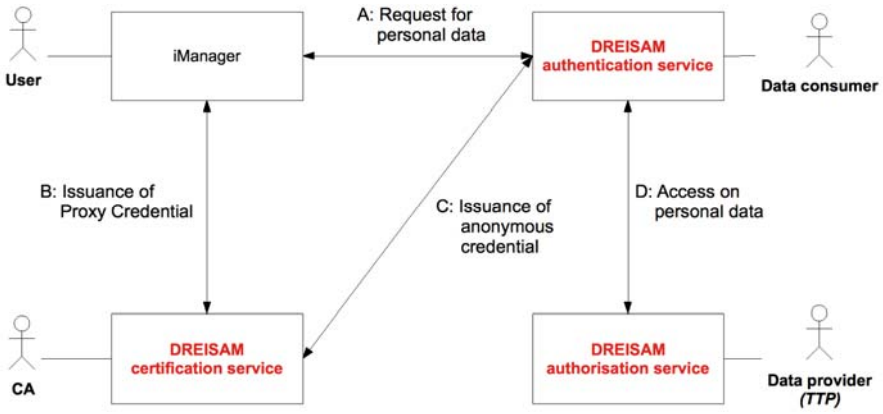

Figure 7.2 The sub services of the DREISAM proof-of-concept implementation

7.2.3 Evaluation of DREISAM

To proof the functioning of DREISAM, one has to show the following properties:

(a) DREISAM does not disclose any identifying data of the user,
(b) the transactions of a user cannot be linked,
(c) the request of a user respectively of a data consumer is accountable, and
(d) a data consumer is only able to use a user's personal data according to the purpose of the corresponding business process.

The cases (a) and (b) refer to a controlled disclosure of personal data; whereas the cases (c) and (d) are about misuse prevention. Since DREISAM makes use of the identity manager iManager, a user is able to decide case-by-case on the disclosure of his personal data by using partial identities. Non-linkability of transactions is achieved by using transaction pseudonyms and anonymous credentials. Non-repudiation of a user for a delegation is achieved by showing his identity and access rights via anonymous credentials and by the log in the delegation list of the CA. Non-repudiation of a data consumer is achieved by showing an anonymous one-show credential to the data provider and by the access log of the data provider. DREISAM enables a user to delegate specific personal data to a data consumer by using proxy credentials. This empowers a user to delegate least authorisation necessary required by a data consumer. The de-anonymisation mechanism of IBM idemix is used for revealing the identity of a user or the data consumer in case of fraud.
It is assumed that the data provider, in case of CRM, follows the obligations of delegated rights and enforces them accordingly. Double-spending of an anonymous one-show credential is detected, if the data provider checks on-line with a CA whether the provided credential has already been used. In the off-line case, such a double-spending cannot be prevented but it can be detected afterwards by the same way as in the on-line case. With respect to undesired re-delegation of a proxy credential, the CA would issue an anonymous credential for another data consumer, which is not mentioned in user's policy. It follows that CA does not follow the certification policy and is not trustworthy. This contradicts the assumption of a trustworthy CA.

Disputes between a user and data consumers relating to the use of access rights may occur in two cases. A data consumer uses a delegated credential and denies its use or a dishonest user uses a credential in the name of a data consumer and denies its use. A dispute is solved by a data provider based on the transcript of the access decisions and on a CA's transcript of a delegation transaction. The data provider compares the transcript of the credential usage with the transcript of issued credentials to identify the cheater.

Thus, DREISAM enables users to control the dissemination of their personal data. Compared to former approaches, the user needs to trust only the loyalty program provider, but not all merchants participating in the loyalty program. Thus, the trust base could be dramatically decreased.

However, the loyalty provider remains a potential weak link. DREISAM does not provide a mechanism to control the loyalty partner. To counter this problem, Section 7.3 presents a mechanism for secure logging, which can be used by the provider to show to its customer that the policies are respected.

7.3 Trusted Virtual Domains (TVD)

Recent advances in IT and business security modeling has yielded to the concept of Trusted Virtual Domain (TVD) (Bussani et al., 2005; Katsuno et al., 2006) which leverages the combination of Trusted Computing and virtualization techniques in order to create a virtual and isolated computing environment that is hosted by several physical platforms. Virtualization techniques allow instantiation of *Virtual Processing Elements* (VPEs, e.g. Virtual Machines[37]) which run as separate processes with own operating system (e.g. Windows, Linux, etc…), sharing the resources of the underlying physical platform (e.g. client's laptop). Those VPEs are isolated even if running on the same platform, and can be subject to security checks (e.g. by means of integrity measurements). A TVD provides a confinement boundary around a set of VPEs no matter if they are running on the same platform or on separate platforms. The TVD establishes trust between member VPEs, and isolates those VPEs from other non-member VPEs even if they share the same platform. Furthermore, it allows enforcement of a domain-wide policy mandating trustworthy security configurations.

[37] Virtual Machines are separate processes which share the underlying physical machine resources, each running its own operating system.

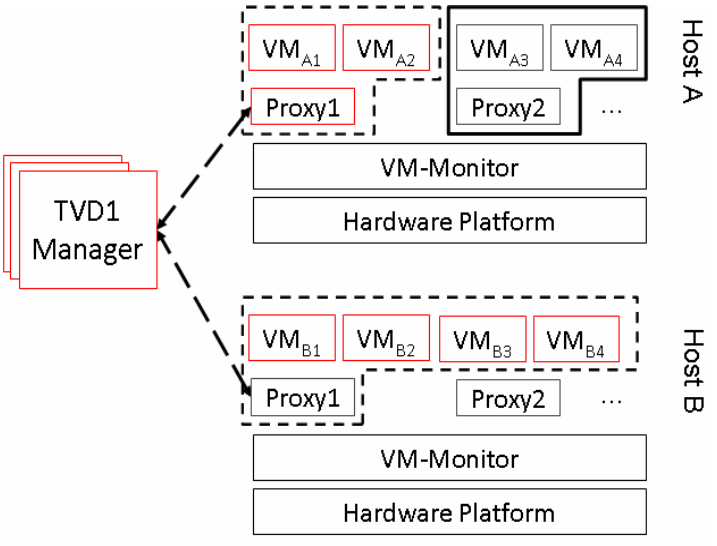

Figure 7.3: Trusted Virtual Domain Model

Typical usage scenarios of TVDs can be found in enterprises, wherein employees perform different tasks under different roles, for example accessing the internet, using intranet services, editing classified documents, and accessing stored private information of users. Each of these tasks has different security requirements. In security-critical environments such as government and military institutes, classified documents are isolated by using physically separated computing platforms. However, in typical enterprise environments users perform these tasks using one computing platform providing a questionable isolation between them. In such an environment, employees could intentionally or unintentionally bypass security policies by sending private information unencrypted over an insecure network connection, or by exchanging private data using an USB stick.

7.3.1 TVDs for privacy

TVDs allow enforcement of a *mandatory security policy* (Gasson, Warwick, 2007) by means of a combination of virtualization techniques and Trusted Computing technology. The confidentiality of privacy-critical information is guaranteed no matter on which physical platform this information is stored or processed as long as this happens within VPEs which are member of the TVD. Moreover, the confidentiality of this data is transparently achieved during transportation of this information between platforms which are part of the TVD infrastructure (client platforms, servers, etc…).

According to D14.3, the requirements for a secure and privacy-enhancing technical infrastructure to provide a verifiable processing of data within a business processes are:

1) Identification of a collection of personal data contrary to the agreed privacy policy.
2) Preventing storage and delegation of personal data if this is in conflict to the agreed privacy policy or at least generating an unmodifiable transcript of these activities.
3) Preventing undesired usage of personal data, i.e. the usage of data the customer has not agreed to.

4) A user must be able to verify whether this monitor is part of the information system and whether applications concerning the processing of personal data are controlled by this monitor.

TVDs help addressing at least the last three requirements. Taking the example of personalized services (cf. D14.3, 3.3) where Service Providers should collect, store and process privacy-critical information about clients, a TVD-based infrastructure can help achieve the basic security requirements which are necessary for protection of this information. The clients will be able to trust the SP for correct handling and non-leakage of information about them due to the following aspects:

- Isolation of their data in a virtual realm (spanning across all platforms, servers and other physical entities at the SP side) which is dedicated for private clients' information.
- Controlled information flow of this private data between trusted entities belonging to the SP.
- Secure processing of and access to the private data by the SP's employees due to access control mechanisms required within the TVD.
- Proof of trustworthiness of the SP's TVD infrastructure to the client himself or to a TTP (usually the TVD-Master).

The TVD-master (a central entity controlling the establishment of the TVD infrastructure on the SP's platforms) can use Trusted Computing techniques to "attest" to the client the software stack which is deployed on each of the SP's platforms where private information is processed. For example, as mentioned in D14.3, Enterprise Rights Management functionality might be necessary for a continuous run-time monitoring of the customer private information usage in a way to prevent misuse of information according to the privacy policy as opposed to controlling the access to the information. With ERM, different roles within the partner enterprise have different fine-grained usage rights over the information. In addition to an access control model, an ERM solution can help controlling the customer information usage by making some information fields accessible to particular persons or roles within the partner enterprise. Such ERM functionality would be part of the software stack, and can be verified for its integrity and availability on the SP's platforms within the TVD (Gasmi et al., 2008).

7.3.2 Organisational Privacy Policy and TVDs

In the following, we take an example privacy policy agreed on between a service provider (for websites (Privacy Policy Examples, 2008) and its costumers, and we include the corresponding TVD specifications that would help enforce such a privacy policy.

Privacy Aspect	Organisational Privacy Policy	TVD Specifications
What information is collected by SP	▪ Name ▪ Mailing address ▪ Email ▪ Phone number ▪ Credit card information	▪ PII collected by a secure application running within the TVD, and which has verifiable trustworthiness.
What the information is used for.	▪ personalised experience ▪ improve customer service ▪ process transactions ▪ administer a survey ▪ send update emails regarding order	▪ *Outside the scope of technical enforcement of policy; can be verified by clients' experience.*
How the information is protected	▪ security measures ▪ secure server, SSL ▪ encrypted in database ▪ access control by employees with specific access rights ▪ private/sensitive data deleted after transaction	▪ Encryption of PII stored on harddrives, external disks (USB) belonging to the TVD. ▪ Encrypted communication between platforms and servers belonging to the TVD. ▪ ERM components on the employees' platforms to enforce fine-grained access control to private data according to access rights.
Cookies usage	▪ used by the SP by default ▪ can be turned off by the user browser settings	▪ Cookies saved only within the TVD compartments on the client's platform.
Disclosing information to outside parties	▪ no selling, trade, transfer of private info ▪ Exception: TTPs who support in service operation ▪ TTPs "should" agree to keep data confidentiality	▪ TTP platforms are part of the TVD ▪ TTP platforms are able to attest the integrity measurements of their software (Trusted Computing).

Table 7.1.: Privacy by TVDs

7.4 Conclusion

A multitude of mechanisms are available today to help to preserve user's privacy even in business processes, where personal data is given away. However, the underlying trust models and assumptions do not allow to rely entirely on those mechanism. Especially, the recent cases of privacy violations shown in Section 5.3 make clear how limited a pure technical approach is.

8 Conclusion and Outlook

Today, personalized services, eGovernment and eHealth application require and process an important amount of personal data. Advances in communication infrastructure, standardisation and "pervasive technologies" (such as for example RFID) make such such intra- and inter-organisational business processes possible. The advantages are obvious and have often been discussed (Strücker, Sackmann, Accorsi, 2006). However, the data owner's right to control the dissemination and the usage of their data (EU Directive, 1985) is difficult to enforce in such settings and thus privacy concerns are considered as the main hurdle for the success of those personalized services (Strücker, Sackmann, Accorsi, 2006). To fully exploit the organisational and commercial possibilities arising from those business processes, technical and organisational means are needed to preserve the users privacy as required by the EU Directive (EU Directive, 1085). This study shows the privacy threats in business processes, the legal requirements and organisational and technical solutions to the privacy threats.

Using the eHealth domain as example, we we show how personal data is shared among business partners within a domain. Unwanted disclosure and unwanted dissemination of personal data happens often and on a large scale. The real cases of the call centres and the lottery company, as well as the case of the German mobile phone provider show that privacy violation happen often and on a large. The analysis shows that mainly missing experience and the lack of precaution paired with insouciance were the main reasons for these debacles. The legal regulations were not neither able to prevent or to sanction the misuse in an appropriate way. On the organisational level, severe faults happened as well. The impact of organisational means therefore cannot be overestimated, together with correctly working and reliable technical mechanisms.

Full technical control if service providers adhere to the privacy policy will be probably unfeasible. With the support of Trusted Computing (TC), as a trustworthy base, transparency enhancing mechanism, such as the logging, will help users to track the usage of their personal data. Today, a set of methods and mechanisms are available for usage control. This range from client-centric identify management systems and their extensions such as DREISAM and tools such as Data Track to the provider side, where methods for private information retrieval for example are available to preserve the users privacy.

The future challenge seems not only the development of more tools and mechanism or the creation of new organisational standards or stronger legal requirements, but to put all those pieces together in order to achieve – depending on the scenario and the application – a coherent privacy architecture consisting of legal, organisational and technical aspects.

9 Bibliography

Accorsi, A., *Automated Counterexample-Driven Audits of Authentic System Records* , PhD Thesis, Albert Ludwig University Freiburg, Germany, 2008.

Anderson, R., *Security Engineering*, Wiley, 2001.

Ball, K., Lyon, D., Wood, D. M., Norris, C., Raab, C., *A Report on the Surveillance Society: Full Report*, http://www.ico.gov.uk/about_us/news_and_views/current_topics/Surveillance. 2006.

Bishop, M., *Introduction to Computer Security*, Addison-Wesley, 2005.

Brückner, L., Voss, M., "MozPETs – a privacy enhanced Web Browser", in *proceedings of the Third Annual Conference on Privacy, Security, and Trust* (PST 2005), St. Andrews, October 2005.

Buitelaar, J. C., Meints, M., van Alsenoy, B. (eds.), *FIDIS Deliverable D16.1: Conceptual Framework for Identity Management in eGovernment*, Frankfurt a.M., 2008. Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp16-del16.1-conceptual_framework_for_identity_management_in_egovernment.pdf

Buitelaar, J. C., Kindt, E. (eds.), *FIDIS Deliverable D16.3: Requirements for privacy-friendly identity management in e-government*, to appear April 2009, Frankfurt a.M. 2009.

Bussani, A., Griffin, J. L., Jasen, B., Julisch, K., Karjoth, G., Maruyama, H., Nakamura, M., Perez, R., Schunter, M., Tanner, A., Doorn, L. V., Herreweghen, E. V., Waidner, M., and Yoshihama, S.; Trusted Virtual Domains: Secure Foundations for Business and IT Services. Technical Report Research Report RC23792, November 2005.

Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Compliance With Canadian Data Protection Laws: Are Retailers Measuring Up?", 2006. http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf

Canadian Internet Policy and Public Interest Clinic (CIPPIC), "How Detailed Information About You Gets Into The Hands Of Organizations With Whom You Have No Relationship", 2006. http://idtrail.org/files/ExecSum_DB.pdf

Eifert, D., „Wert von Kundenprofilen im Electronic Commerce“, *Electronic Commerce*, Vol. 28. Lohmar. Cologne. 2004.

Ellison, C., Frantz, B., Lamspon, B., Rivest, R., Thomas, B., Ylonen, T., “SPKI Certificate Theory”, *Internet Request for Comments 2693*, Network Working Group, 1999.

European Commission: Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L281, p. 31–50, 1995.

Franklin, M., ”A survey of key evolving cryptosystems”, *International Journal of Security and Networks* Vol.1 No1/2, pp.46–53, 2006.

Gasmi, Y., Sadeghi, A., Stewin, P., Unger, M., Winandy, M., Husseiki, R., Stüble, C., „Flexible and secure enterprise rights management based on trusted virtual domains”, in *Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing* (Alexandria, Virginia, USA, October 31 - 31, 2008). STC '08.

Gasson, M., Warwick, K. (eds.), *FIDIS Deliverable D12.2: Study on Emerging AmI Technologies*, Frankfurt a. M., 2007. Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-d12.2_Study_on_Emerging_AmI_Technologies.pdf

German Federal Government: German Teleservices Data Protection Act, 1997.

Glynos, D., Kotzanikolaou, P., Douligeris, C., ”Preventing impersonation attacks in MANET with multi-factor authentication”, Proceedings of the 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp.59–60, *IEEE Computer Society Press*, 2005.

Hildebrandt, M. (ed.), FIDIS Deliverable 7.12: “Biometric Behavioural Profiling and Transparency Enhancing Tools”, to appear. Simone Fischer-Hübner and Hans Hedbom (eds.), PRIME Deliverable 14.1: Framework V3, http://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.c_ec_wp14.1_v1_final.pdf (last visited: February 22, 2009).

Hildebrandt, M., Meints, M. (eds.), *FIDIS Deliverable D7.7: RFID, Profiling, and AmI*, Frankfurt a. M., 2006. Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.7.RFID_Profiling_AMI.pdf

Howard, M., Leblanc, D., "Writing Secure Code", *Microsoft Press*, 2001.

Initiative D21, *IT-Sicherheitskriteriensysteme im Überblick*, Bonn, Germany 2001.

Katsuno, Y., Kudo, M., Perez, P., Sailer, R.; Towards Multi-Layer Trusted Virtual Domains, the 2nd Workshop on Advances in Trusted Computing, 2006.

Kenneally, E., "Digital logs – Proof matters", *Digital Investigation*, Vol.1, No.2, pp. 94–101, 2004.

Kent, K., Souppaya, M., "Guide to Computer Security Log Management", National Institute of Standards and Technology (NIST), September 2006.

Kohl, J., Neuman, C., "The Kerberos Network Authentication Service (V5)", *Request for Comments 1510*, 1993.

Lamport, L., "Password authentication with insecure communication", *Communications of the ACM*, Vol. 24, No.11, pp.770–772, 1981.

Langheinrich, M., „Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie", in Fleisch, E., Mattern, F. (eds.): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, pp. 329–362, Springer, 2005.

Lam, S. K., Frankowksi, D., Riedl, J., "Do You Trust Your Recommendation? An Exploration of Security and Privacy Issues in Recommender Systems", in Proceedings of Emerging Trends in Information and Communication Security (ETRICS) 2006, *Lecture Notes of Computer Science*, Vol. 2995. pp. 14–29, Springer, 2006.

Meints, M., "Effektives Datenschutzmanagement unter Nutzung von IT-Betriebsprozessen", *Datenschutz und Datensicherheit*, vol. 29, no. 10, pp. 588–591, Wiesbaden 2005.

Meints, M., "Datenschutz und IT-Grundschutz", *kes*, vol. 2007, no. 5, pp. 59–62, Ingelheim 2007.

Meints, M., (2007a) "Datenschutz durch Prozesse", *Datenschutz und Datensicherheit*, vol. 31, no. 2, pp. 91–95, Wiesbaden 2007.

Meints, M., "The Relationship between Data Protection Legislation and Information Security Related Standards", to appear in "Proceedings of the FIDIS/IFIP Summer school 2008", *Lecture Notes in Computer Science*, Springer-Verlag, Heidelberg 2009.

Meints, M. (2009a), „Die Datendiebstahlskandale des Jahres 2008 – Was wir im Sicherheitsmanagement daraus lernen können“, to appear in *Datenschutz-Berater* 03/2009, Fachverlag der Verlagsgruppe Handelsblatt, Düsseldorf 2009.

Meints, M. (2009b), “Musterprozesse für das Datenschutzmanagement”, *IT-Grundschutz Infordienst* 1/2009, p. 12–15 and 2/2009, Ingelheim 2009.

Meints, M., „Protokollierung bei Identitätsmanagementsystemen – Anforderungen und Lösungsansätze“, in *Datenschutz und Datensicherheit – DuD*, Vol. 30, No. 5, May 2006, Vieweg Verlag.

Müller, G., Wohlgemuth, S., (eds.), *FIDIS Deliverable D14.2: Study on Privacy in Business Processes by Identity Management*, Frankfurt a. M., 2007. Download: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp14-del14.2-study_on_privacy_in_business_processes_by_identity_management.pdf.

Pettersson, J. S., Bergmann, M., Fischer-Hübner, S., *Outlining Data Track: A Privacy-friendly Data Maintenance Approach for End-users*, presented at ISD 2006, Fifteenth International Conference on Information Systems Development, Budapest, August 2006, Springer Verlag.

Pretschner, A., Hilty, M., Basin, D., “Distributed usage control”, in Communications of the ACM 49(9). Special Issue: Privacy and security in highly dynamic systems, pp. 39–44, *ACM Press*, 2006.

Prosser, W., “Privacy”, California Law Review 48, pp. 383–423, 1960.

Privacy Policy Example - Template, WebsitePrivacyPolicy.com, http://www.website-privacy-policy.com/privacy-policy.html, 2008

Rannenberg, K., Pfitzmann, A., Müller, G., “IT Security and Multilateral Security”, in Multilateral Security in Communications - Technology, Infrastructure, Economy, pp. 21–29. Addison-Wesley-Longman, 1999.

Simon, C., „Arbeiten zum Datenschutz im IT-Grundschutz vorläufig abgeschlossen“, *Datenschutz und Datensicherheit*, vol. 31, no. 7, p. 486, Wiesbaden 2007.

Solove, D. J., "The Digital Person: Technology and Privacy in the Information Age", *New York University Press*, 2006.

Strüker, J., Sackmann, S., "New Forms of Customer Communication: Concepts and Pilot Projects", in Proceedings of the 10th Americas Conference on Information Systems (AMCIS '04) USA, 2004.

Weichert, T., „Der Skandal um den Datendiebstahl und seine Folgen", *FIfF-Kommunikation* 4/2008, pp. 5–9, Bremen 2008.

Welch, V., Foster, I., Kesselmann, C., Mulmo, O., Pearlman, L., Tuecke, S., Gawor, J., Medder, S., Siebenlist, F., "X.509 Proxy Certificates for Dynamic Delegation", in 3rd Annual PKI R&D Workshop, 2004.

Zugenmaier, A., "Anonymity for Users of Mobile Devices through Location Adressing", RHOMBOS-Verlag, 2003.

10 Annex 1: Glossary

ALE	Annual Loss Expectancy
BDSG	Bundesdatenschutzgesetz, the German Federal Data Protection Act
CC	Common Criteria
CMDB	Configuration Management Database
CobiT	Control Objective for Information and related Technology
CRMS	Customer Relationship Management System
DPMS	Data Protection Management System
DPO	Data Protection Officer
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	IT-Infrastructure Library, a collection of good practice processes for IT service management
PMM	Process Maturity Model
SLA	Service Level Agreement
SLO	Single Loss Occurrence
SSLA	Security Service Level Agreement
TAN	Transaction Number
USB	Universal Serial Bus