
Collaborative Project



Integrated Project Reflective Learning at Work

European Commission Seventh Framework Project (IST-257617)

Deliverable ***D9.1***

User studies on privacy needs, privacy model and privacy guidelines

Editor *Martin Degeling, Roy Ackema*

Work Package *WP9*

Dissemination Level *Public*

Status *Draft*

Date *02-May-2011*

The MIRROR Consortium

Beneficiary Number	Beneficiary name	Beneficiary short name	Country
1	imc information multimedia communication AG	IMC	Germany
2	Know-Center (Kompetenzzentrum für wissensbasierte Anwendungen und Systeme Forschungs-Und Entwicklungs GmbH) Graz	KNOW	Austria
3	Imaginary srl	IMA	Italy
4	Deutsches Forschungszentrum für Künstliche Intelligenz GmbH Saarbrücken	DFKI	Germany
5	Ruhr-Universität Bochum	RUB	Germany
6	The City University	CITY	UK
7	Forschungszentrum Informatik an der Universität Karlsruhe	FZI	Germany
8	Norges Teknisk-Naturvitenskapelige Universitet	NTNU	Norway
9	British Telecommunications Public Limited Company	BT	UK
10	Tracoin Quality BV	TQ	Netherlands
11	Infoman AG	INFOM	Germany
12	Regola srl	REG	Italy
13	Registered Nursing Home Association Limited	RNHA	UK
14	Neurologische Klinik GmbH Bad Neustadt	NBN	Germany
15	Medien in der Bildung Stiftung	KMRC	Germany

Amendment History

Version	Date	Author/Editor	Description/Comments
V0.1	02-May-2011	RA	First version
V0.2	01-June-2011	MD	Version for Peer Review
V1.0	29-June-2011	MD	Version for submission

Contributors

Name	Institution
M. Degeling	RUB
M. Prilla	RUB
R. Ackema	TQ

Reviewer

Name	Institution
Birgit Krogstie	NTNU
Anne König	INFOMAN

Legal Notices

The information in this document is subject to change without notice.

The Members of the MIRROR Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the MIRROR Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Executive Summary

The objective of the trust and privacy related work of WP9 in year one was to conduct empirical studies to identify concerns and possibilities regarding data protection and disclosure.

In the next project year this objective will expand into development of concepts of data manipulation and disclosure to reduce risks both at the technical and organisational level.

This deliverable describes the results of the empirical studies carried out to identify concerns regarding data protection and disclosure with respect to the applications created within the project.

To support individual, collaborative and organisational reflection it is anticipated that users share (captured) data from work processes as well as data that is created during reflection processes (e.g. annotations as articulations of reflection outcomes). This is on the one hand a question of privacy needs but on the other a question of sharing culture and trust between employees as the underlying mechanism.

For the user studies we identified four aspects related to privacy and trust to focus on:

- *Sharing behaviour*, which, we assume, differs from the first mentioned concerns since trust with its non-conscious components has some influences apart from the decision individuals make concerning privacy.
- *trust in organisation*, where the organisation is represented on the one hand by supervisors and manager who can reward or punish certain behaviours and on the other by operators of applications used within MIRROR
- *trust in other users*, as direct colleagues and members of the same team who are seen as reflection partners and therefore later may get deeper insights into the data captured by MIRROR apps.
- *individual concerns* resulting from user dependent attitudes of how sensitive they think their personal data is and how it should be handled.

Based on these distinctions we developed a survey to explore these aspects and their relationship.

The survey was carried out at all five test-beds of the MIRROR project. In total 133 participants completed the survey.

After analyses of the data we have derived the following conclusions:

a) *Individual concerns about privacy is not directly related to real sharing behaviour*

We found no direct relations between the measured privacy concerns and the way people share personal data that can be generalized. Results from one testbed indicate that there might be a correlation between sharing and one aspect of privacy concerns, unauthorized secondary use of the data, but this has to be further investigated to be verified.

b) *Sharing behaviour is related to trust in colleague*

We could not generally approve this relation but found a correlation at NBN between answers to the questions “I talk to my colleagues about personal things” and “I fully trust my colleagues [...]” which could not be confirmed by data from the other testbeds. This indicates a relation which has to be taken into account.

c) *Sharing behaviour is related to trust in the organisation*

We found no correlation in support of this in our dataset. This may be related to our questionnaire which asked about sharing with colleagues, and not explicitly sharing with the organisation. An interpretative explanation is that in working environments staff thinks about sharing with colleagues where effects are more direct visible and not about the organisation perhaps of system complexity.

d) *Trust in colleagues is related to willingness to share data with them*

As described above there is a relation between trust in colleagues and the willingness to share personal data, at least for the testbeds where the full-length questionnaire was conducted. The implication for MIRROR is that we have to take trust relationships into account.

e) *Trust in organisation is related to willingness to share data with the organisation*

This relation is indicated by the data of all but RNHA. Together with the strong refusal of secondary use of data for other purposes and dependent on the trust in the organisation, this implies a greater need for security mechanisms to prevent misuse by the organisations.

The following conclusions are derived as recommendations for the MIRROR project:

- Since there is a strong refusal of secondary usage of data although participants trust their organisation we see a need to enforce data security mechanisms especially **confidentiality** to ensure MIRROR app users are in control of who has access to their data.
- The very individual view on privacy and concerns about it can be seen as a need for **transparency** with respect to which data is available as well as what happens with it. This would not only be to support users in their rights to be in control and therefore gain trust, but would also foster awareness about when the data they share helps others and keep track about how reflection outcomes are implemented in their work practice. Transparency mechanisms can also support building of trust relations especially towards the organisation since it is comprehensible for users how their personal information is used.
- Since some users have higher personal standards and privacy concerns than others independent of the testbed they are working in we recommend mechanisms of **adjustability** to allow individual settings according to user needs. Also trust is a flexible and changes over time. Therefore models for Access Control Policies (ACP) have to be developed that on the one hand fit users' needs and on the other are easy to use.

To support the development of the first version of the MIRROR architecture and MIRROR apps this deliverable also describes possible technical and procedural solutions to safeguard the privacy of users of these apps.

Table of Contents

1	Introduction	8
2	Background	9
2.1	Theoretical Background	9
2.2	Technical Background	10
2.3	Legislative Background	16
3	Research Interests and research approach	19
4	Testbeds and sample	21
4.1	Descriptions of the Testbeds	21
5	Methods and research instruments	24
6	Data analysis and results	26
6.1	Analysis of descriptive statics	26
6.2	Analysis of correlations	30
7	Overview and recommendations	33
7.1	Recommendations from user studies	33
8	Appendix A: Guidelines for Actions to Safeguarding the Abuse of Personal Data Collected with Mirror Apps	34
8.1	Data classification	34
8.2	Overview of the actions by type of data	35
9	Appendix B: Privacy Questionnaire	38
	References	41

Table of Figures

Figure 1: Model of asymmetric encryption	13
Figure 2: SAML 2.0 Authentication Process	15
Figure 3: XACML Actors and Data flow	16
Figure 4: Averages of answers to questions about trust in colleagues; 5 = strongly agree; 1 = strongly disagree.	26
Figure 5: Averages of answers to questions about willingness to share. 5 = strongly agree; 1 = strongly disagree.	27
Figure 6: Averages of answers to questions about trust in colleagues. 5 = strongly agree; 1 = strongly disagree.	28
Figure 7 Averages of answers to questions about trust in colleagues. 5 = strongly agree; 1 = strongly disagree.	28
Figure 8: Averages of answers to questions about general privacy concerns. 5 = strongly agree; 1 = strongly disagree.	29

1 Introduction

Privacy and security in software systems are core concepts of each software development project not only to comply with legislation but to make software systems robust against attacks and gain the trust of employers as well as users of the system.

In the first part of this deliverable, trust and privacy within MIRROR are described from different angles. First, from a theoretical side we take a look at the various implications of trust and privacy in work environments. Second, we describe a technical perspective and give a brief overview of current approaches and problems that exist for privacy and security in software systems and that ought to be addressed during the development of a MIRROR-Architecture. And third, we take a look at legislative issues related to privacy in work environments.

The second part of this deliverable describes user studies of WP9 conducted within the MIRROR testbeds to gain insights into how privacy is perceived in the testbeds and what possibilities participants see for data sharing for reflection. To collect data we developed a questionnaire covering different privacy perspectives such as data sharing, willingness to share under different circumstances, trust in colleagues, trust in the organisation and general privacy concerns. The results of this questionnaire are presented in chapter 6.

2 Background

2.1 Theoretical Background

To support individual, collaborative and organisational reflection it is necessary that users share (collected) data as well as data that is created later in the reflection process (e.g. annotations as articulations of reflection outcomes). This is on the one hand a question of privacy needs but on the other a question of the sharing culture and trust that exists.

In groups that rely on interaction and collaboration that is not heavily formalized as we assume in MIRROR, trust is an important factor that simplifies coordination between group members (Herrmann 2001 and Seifert and Pawlowsky 1998). Trust supports cooperative and communicative behavior where formalization and structures are missing, for instance in reflective professions that need cooperation and sharing of data and experience. Two perspectives of trust in organisations are described by Kramer (1999). The first perspective describes trust as a method people use in interaction with imponderability and risks. In situations where they cannot estimate the motives and intentions of an opponent and thus do not know about future behavior, trust is needed. The second perspective describes trust from a calculable, economic view of trade where different factors and knowledge of trade partners are taken into account in a cost-benefit analysis. Every participant in a trade situation could therefore estimate whether it is in their own interest to trade or not. The latter model is heavily criticized because research proved that in trust based interaction there is often a lack of information required to calculate these cost-benefits, and trust is more of a non-conscious decision as described in the first model. According to Kramer (1999) trust has three major benefits:

- complexity of transactions and transaction costs are reduced, allowing quick decisions to be made instead of long economic calculations,
- spontaneous *sociability* between members of an organization is increased since it is easier to comply with organizations' expectations to cooperate if trust is established between employees,
- willingness to participate in a given organizational structure is higher if own and others' decisions do not need to be questioned or controlled every time.

With regard to the last point Iachello and Hong (2007) state that trust is therefore needed not only in technical systems but in all users of the system and their usage of its data according to estimated behavior. Otherwise a technical system is only used in a way that fosters the best possible perception a user wants to show instead of really supporting reflection. In work contexts we further divide these relations into trust in other employees on the same level of hierarchy as well as trust in supervisors or project leaders.

On this basis we differentiate four aspects related to privacy and trust we regard as relevant to MIRROR and which guide the development of the questionnaire:

- *Sharing behaviour*, which, we assume, differs from the individual privacy concerns since trust with its non-conscious components has some influences apart from the decision individuals make concerning privacy.
- *trust in organisation*, where the organisation is represented on the one hand by supervisors and manager who can reward or punish certain behaviours and on the other by operators of applications used within MIRROR

- *trust in other users*, as direct colleagues and members of the same team who are seen as reflection partners and therefore later may get deeper insights into the data captured by MIRROR apps.
- *individual concerns* resulting from user dependent attitudes of how sensitive they think their personal data is and how it should be handled.

Several studies have already found that individual concerns about privacy is not directly related to the real behaviour of users when it comes to revealing and sharing data (e.g. Taylor, 2003, Acquisti and Grossklags, 2005, Cranor et al., 2000) and for social networks (Dwyer et al., 2007). Influences on the behaviour may be short term benefits that convince even users that rated themselves as “privacy fundamentalists”¹ to reveal personal information, especially on e-commerce sites. Other studies indicate that the design (Naone, 2010) or given information provided about how the data will be processed has an effect on the amount of data users are willing to share. This is why WP9 takes a closer look at how data sharing is organized in the testbeds.

Evaluations of trust in the organisation have been designed in other contexts of privacy, e.g. by Dwyer et al. (2007) and Smith et al. (1996). Results of this questionnaire may also influence MIRROR Apps in the way they store data. If the organisation is not trusted it may be useful to keep personal data only on personal devices or apply stronger cryptographic methods to prevent unauthorized usage.

2.2 Technical Background

The following section provides an overview of the technical perspective on privacy and security followed by a description of means that are taken into account when planning the MIRROR Apps and Architecture.

2.2.1 Goals of privacy and security in software systems

In technical discussions about privacy, security mechanisms like encryption are often mentioned as the solution to privacy problems. However, security and privacy goals are comparable but not always congruent. Whereas both aim at protecting data from misuse and theft, security methods are more focused on the data itself and the protection of the software system holding it and privacy methods target at the protection of data subject, the persons and users described by the data throughout the system. This sometimes leads to difficulties: For example, where security methods would log every access to a system in order to e.g. at least be able to identify an attacker afterwards, privacy methods would try to protect even the data logged by these methods or prevent excessive logging.

2.2.1.1 Information Security goals

Common goals in security discourses are (Paar and Pelzl 2010)

- **Confidentiality:** Make sure information cannot be read except by the recipient and prevent the disclosure of information e.g. through encryption.
- **Integrity:** Ensure information is not changed in transition between sender and recipient or at least offer means to detect changes. This can be ensured e.g. by checksums.

1. Other groups are “privacy pragmatists” and “privacy unconcerned” (Westin, 2003)

- **Authenticity:** Make sure that the communication partners on both ends are the ones they claim to be and the information exchanged is genuine. Authentication infrastructures e.g. with user name and password provide this basic functionality.
- **Availability:** To enable information exchange with computer systems the availability of this systems has to be ensured e.g. by providing data backup.
- **Non-repudiation:** Enable information partners to control information flow by making sure information was received and enable mechanisms that do not allow a party to deny a message was sent by them e.g. by establishing secure connections and use of cryptographic signatures.

2.2.1.2 Privacy goals

Rost and Bock (2011) identified some more operationalized methods in the normally more abstract discussion of privacy goals driven by legislation. They identified the needs for

- **Transparency:** This refers not only the verifiability that is required by legislation but also techniques that offer users the abilities to be in control of their personal data by describing rules for what is allowed to happen with it and what is not allowed.
- **Nonchainability:** The request for mechanisms that prevent the merging of different datasets except for purposes where consent of the data subject exists.
- **Interventionality:** For the affected users methods should support the simple interaction with the system to gain control over their data. If internal processes are related to the data, mechanisms have to be applied to avoid failures.

2.2.2 Technical challenges

To comply with these goals of privacy and security in software systems development in MIRROR has to face several challenges.

2.2.2.1 Complexity of configuration

The more options are offered to control access of data the less usable they are to untrained users (Whitten und Tygar 1999). To find the right trade-off between security and usability is not easy and to find the best default setting is a difficult task. Some possible approaches are summed up in Fischer-Hübner, Iacono, and Möller (2010).

2.2.2.2 Inter-application Sharing

Since the growth of the Internet and the rising number of interoperable Web2.0 mash-ups, the sharing of data between apps like those to be developed in MIRROR has continuously been made easier. Unfortunately there is not yet a common framework to ensure that the privacy and security setting of a data object in one application is correctly understood and enforced in other applications as well.

2.2.2.3 Context Sensitivity

In the best case, privacy and security mechanisms not only enforce access rights but also make sure that after access is granted the data is only used in the way intended by the user. A user may, for example, share a personal document with a trusted colleague and allows them to read and maybe even comment on it. In this case there should still be a mechanism to prevent the misuse of data for example by printing or copying it to other programs.

2.2.2.4 Re-calibration of Rules

Any digital information can be copied and retained disconnected from their context. But there are, and should be, mechanisms to make user privacy and security policies evolve together with their social surrounding. These mechanisms, which are explained in the following parts of this chapter, reach from the deletion of data to intelligent adaption of new context settings (e.g. restrict access to my data for a colleague that changed department).

2.2.3 Access Restriction

To meet some of the goals and challenges technical means are needed to ensure only those have access to data that apply to rules and restrictions set by the data owner. The following section describes the state-of-the-art of access control mechanisms.

2.2.3.1 Access Control Policies (ACP)

„An ACP protects access to an object by specifying which subjects should be granted which type of access to it. The object being protected can be a piece of data like a file, a database record, or a web page, but it can also be a more abstract functionality like a service or a remote procedure call.“ (Martin Pekárek 2009)

A comparison of different ACP technologies for groupware and collaboration tools can be found in Tolone et. al. (2005)

Access Control based on Identifiers

Access matrices are a common model for management of access rights. For every object (folder or file) there is an access right for every subject (users) where the access rights are managed on the level of read and write-access. Several operating systems use this scheme with added rights e.g. for execution or for an *owner*-role. Access matrices are not capable of multidimensional rights or inheritance(e.g. Dewan und Shen 1998).

Access Control based on Roles and Groups

Role based access control (RBAC) allows connecting the access rights with a role and privileges assigned to a role instead of a particular user. Roles can be assigned to different and multiple users to allow or restrict access to information. RBAC was be extended by Tolone, Ahn, et. al. (2005)to a system that not only uses roles for users but also for objects. Although RBAC might be a good idea for shared material of a group of users, personal information should be owned and controlled by the users it describes.

Access Control based on Attributes or Context

Context-Awareness Access Control described by different authors (e.g. Langheinrich 2001, Zhang und Parashar 2004 or Bhatti, Bertino, u. a. 2005) makes the access rights dependent on context information like the spatial position of the user trying to access an object, the current time etc. In *Attribute Based Access Control* access is granted dependent on attributes of users like age or special attributes given according to policies, e.g. only employees of a special department that had a security audit are allowed to enter a server room.

2.2.4 Prevent/Secure Access

From data security research there exist various encryption algorithms and protocols to ensure confidentiality of data to prevent unauthorized access or change. Available algorithms that are in use can be categorized as either symmetric or asymmetric.

2.2.4.1 Symmetric encryption

Symmetric encryption is based on a shared secret of the communication partners (here referred to as Alice (A) and Bob (B)). The principle is that Alice as well as Bob has knowledge of a secret (e.g. a passphrase) only the two of them know. With this secret the messages they share with each other are encrypted and decrypted. This principle is used in various broadly accepted algorithms e.g. Data Encryption Standard (DES)² or Advanced Encryption Standard (AES).

2.2.4.2 Asymmetric encryption

Asymmetric encryption addresses the one flaw that comes along with symmetric encryption. Alice and Bob need the ability to exchange the secret they have, and to prevent cryptanalytic attacks they have to do this regularly. Asymmetric encryption algorithms like the *RSA* or *EIGamal cryptosystems* are based on mathematic principles that allow the exchange of encrypted information without a shared secret. To do this Alice sends Bob a public (non-secret) key he and everybody else can use to send encrypted messages to Alice (see Fig. 13). These algorithms are based on mathematical functions that allow easy computation of one way (encryption) with the public key but without knowing the secret key the other way (decryption) requires disproportionately high effort.

Since these asymmetric algorithms require a larger amount of computation, current protocols (e.g. *SSL* for *HTTP*) make use of both encryptions schemes. They use asymmetric encryption to exchange a key that is afterwards used to symmetrically encrypt the rest of the communication.

To choose the right encryption protocols it is necessary to determine the sensitivity as well as other factors. For example, if a message is fully (end-to-end) encrypted between Alice and Bob it is not possible – not even for trusted third parties like the server of the organisation – to use the data for any analysis. Even sharing with multiple communication partners gets more difficult depending on the level of encryption used.

2.2.5 End Access

Data may be deleted after a given time or a given event (for example when a worker leaves the company). This is also requested by the European privacy directive 95/46/EC. To achieve this dynamic handling of disclosure approaches like *vanish* (Geambasu et. al. 2009) and *ephemerizer* (Perlman 2005) allow data objects to “disappear” by making them inaccessible.

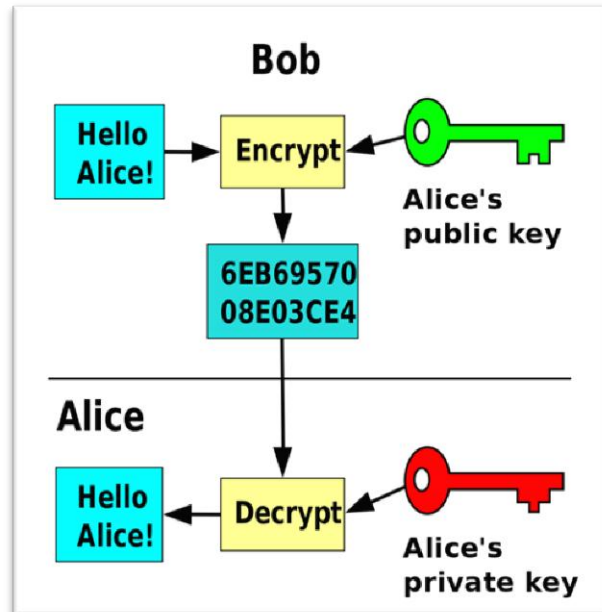


Figure 1: Model of asymmetric encryption

² For an introduction see e.g. Paar and Pelzl (2010)

³ Source: http://en.wikipedia.org/wiki/File:Public_key_encryption.svg

Even if the time for deletion of data is not yet reached there may also be reasons to restrict access because of changes in the organisational structure or based on changed trust relations, e.g. a person quits a team or changes its position inside the team from normal member to supervisor.

2.2.6 Architecture recommendation for data privacy

The methods and mechanisms described above address one or more problems of data security and privacy. The following part of the document describes more high-level approaches for software architecture.

According to Pekárek (2009), access control systems should be able to manage access for groups and individuals in a way reflecting the nature of the relationships in reality; this is called *identity and relationship management*, which can be achieved by *Single-Sign-On* (SSO) and a federated authentication and authorization infrastructure.

To meet these requirements in a complex architecture, the Organisation for the Advancement of Structured Information Standards (OASIS) defined XML-based policy languages and process models.

2.2.6.1 Security Assertion Mark-up Language (SAML)

SAML is an XML-Framework for exchange of authentication and authorization information with a focus on Single-Sign-On to enable the usage of different services with one authentication (e.g. username); this is used for example by some Google services. To make this possible authentication it is no longer implemented on the Service Provider Level but outsourced to an Identity Provider as shown in Figure 2. Besides the Single-Sign-On abilities this architecture has some privacy relevant advantages that allow hiding specific user information from the service provider. If, for example, the authorization of a web service is dependent on the age of a user, the identity provider only needs to authenticate this single attribute of the user (e.g. age>18; yes|no).

Other Single-Sign-On mechanisms with a similar approach that have gained popularity especially for web services are Oauth⁴ and OpenID⁵.

4 <http://oauth.net/>

5 <http://openid.net/>

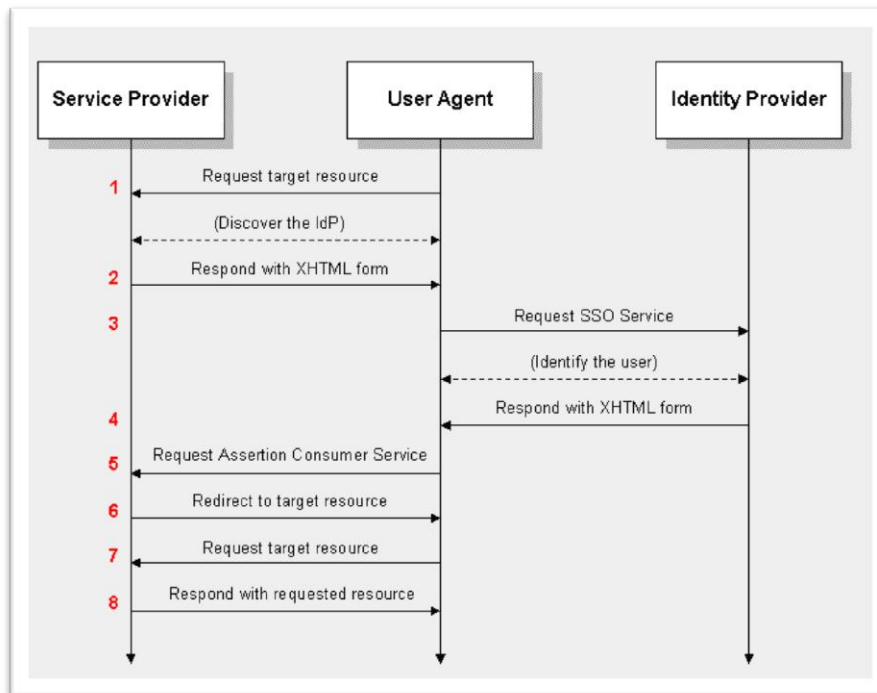


Figure 2: SAML 2.0 Authentication Process⁶

2.2.6.2 Sticky Policies and XACML

In addition, a common user authentication like the one explained above allows a more sophisticated access management approach. *Sticky policies* meet some of the goals described in 2.2, especially re-calibration of rules and access restriction. The idea is that every data set has a policy attached that defines rules for usage, for example who might access the data in which context and for how long. These are pieces of information tied to a data object by digital signatures and encryption in contrast to approaches where access restriction is controlled by a separate unit that stores access rules with a relation to the data object. Cryptographic grounding and rudiments for Key Management are described by various authors, e.g. Ardagna, De Capitani di Vimercati, et. al. (2006), Nepal, Zic, et. al.(2009) and Dürbeck, Kolter, et. al. (2010). Currently there is are European project like Tas³, PrimeLife or Nessi/Nexof⁷ working on architecture models and simple ways of implementation.

Among the widely used standard for defining policies for data objects that include obligations and handling conditions is the *eXtensible Access Control Markup Language (XACML)*.

With XACML both privacy and security policies can be expressed in a machine-readable language. XACML is being developed by the OASIS XACML Technical Committee.

To enforce the policies in service oriented architecture the XACML Infrastructure consists of several entities as shown in Figure 3.

- Policy Enforcement Point (PEP) - Point which intercepts the user's access request to a resource and enforces PDP's decision.
- Policy Decision Point (PDP) - Point which evaluates and issues authorization decisions

⁶ Source: http://en.wikipedia.org/wiki/SAML_2.0

⁷<http://www.tas3.eu>; <http://www.primelife.eu>; <http://www.nessi-europe.com/>

- Policy Administration Point (PAP) - Point which manages policies
- Policy Information Point (PIP) - Point which can provide external information to a PDP, such as LDAP attribute information.

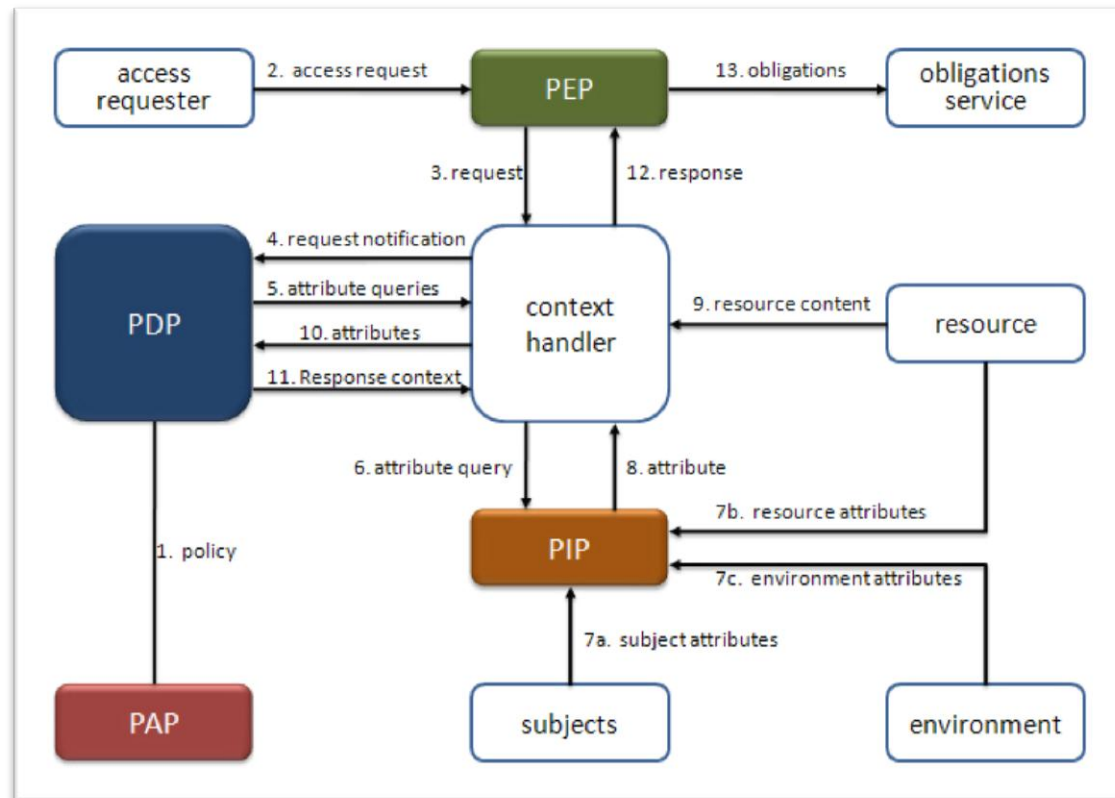


Figure 3: XACML Actors and Data flow⁸

2.3 Legislative Background

Besides technical means to enforce privacy there are legislative issues with which the MIRROR Apps have to comply. This legislation does also apply at workplace. On the one hand there is a European directive stating a framework of rules and on the other hand every member state of the European Union has separate, sometimes more restrictive, laws for data protection and privacy.

2.3.1 Regulations

The protection of personal data within Member States of the European Community is regulated by the European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995]. The main objectives of the directive are:

1. "In accordance with this Directive, Member States shall protect the fundamental rights and freedom of natural persons and in particular their right to privacy with respect to the processing of personal data.

⁸ Source: <http://www1.cse.wustl.edu/~jain/cse571-09/ftp/soa/index.html>

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.“

2.3.1.1 National Law applicable

The user studies of WP 9 take place at the MIRROR testbed partners from the United Kingdom (BT and RNHA), Germany (INFOM and NBN), and Italy (REG). **Fout! Verwijzingsbron niet gevonden.** gives an overview of the laws that apply in the EC Member States where MIRROR partners are located.

Each organisation may have its own policies for the treatment of personal data of their employees or related individuals in addition to any local laws that apply. Company policies cannot however conflict with EU or National Laws. Sometimes, however, organisational policies and regulations are more specific and refer to the existing technologies and practices while the law tends to be more general.

Table 1: Overview of data protection laws that apply in the EC member states of MIRROR partners

Member State	MIRROR Partner	Law
United Kingdom	BT, RNHA, CITY	Data Protection Act
Italy	REG, IMA	Codice in materia di protezione de idatipersonali
Germany	INFOM, NBN, IMC, DFKI, RUB, FZI, KRMC	Bundesdatenschutzgesetz and federal laws
Austria	KNOW	Datenschutzgesetz 2000, and Landesdatenschutzgesetz 2001 (federallaw, Styria)
Norway	NTNU	Personal Data Act of 2000
The Netherlands	TQ	Wet Bescherming Persoonsgegevens

2.3.2 Common principles

It is beyond the objective of this deliverable to give a detailed summary of the provisions of the above mentioned laws. However we found the underlying principles in these laws to be very similar (as an expected consequence of the EU directive). Therefore we have identified the following common principles on which we will base our guidelines for handling personal data within the MIRROR appsphere:

1. Fair and Lawful processing (Consent)

- Data collection should be conducted according to local privacy principles and laws.
- Consent has to be signed by the data subjects using MIRROR apps.

2. Specified purpose

- Tell the data subject about with whom the data will be shared and what the purpose of the data collection is.
- When using the data, researchers should be aware of the purpose for which the data was collected.
- Specified purpose also means no disclosure to third parties outside the MIRROR Group.

3. Do not keep more data or keep it longer than necessary
 - Personal information should be deleted or made pseudonymous or anonymous if possible within the apps (for definitions of pseudonym and anonym see Pfizmann A, Hansen M., 2010).
 - The data should not be kept longer than necessary for the purpose it is needed.
4. Data subjects' rights
 - The data subjects should have the right to access and correct the data if requested.
5. Security
 - Data should be handled proportionately to the sensitivity of the data throughout the whole processing.
6. Control and responsibility
 - A responsible data protection commissioner for the MIRROR appsphere has to be specified who is in charge of data usage and changes of purpose. This person should also be the contact person for data subjects that want to know what is stored about them or have other concerns.

This chapter summarized three perspectives of privacy that have to be taken into account for development of MIRROR. First, we described aspects of interpersonal trust and trust towards the organisation as a basis for cooperation and data sharing within technical systems. Second, we proposed technical standards for privacy and security, and third, we provided an overview of issues of legal compliance with regard to privacy. Whilst the third perspective offers a baseline in the form of regulation and needs more specification in workplace settings there is a range of possibilities to achieve this technically. Which solution serves MIRROR best is dependent on the concrete privacy needs of the testbeds and their perceived trust relations. To get deeper insights about what the perceptions of privacy and trust are in the MIRROR testbeds we conducted a survey for the user studies of MIRROR which will be described in the following chapters.

3 Research Interests and research approach

The user studies of WP9 are focussed on the privacy needs of the testbeds. We wanted to identify privacy concerns in the testbeds as well as the current sharing behaviour in order to inform application development in each testbed. Additionally we wanted to analyse the influence of trust between individuals and towards groups and organisation on the privacy concerns and sharing behaviour in order to use these results later to develop guidelines for a privacy and security model of the MIRROR appsphere. In addition, results from both analyses were meant to add to the theory of reflection support developed in MIRROR by informing it about sharing behaviour, opportunities and constraint. For this we outlined four aspects of privacy and trust described in section 2.1. These more general aspects were incorporated into a questionnaire⁹ with 26 questions covering the question topics stated above. Concrete questions were based on questionnaires with a similar focus conducted and evaluated by other researchers. In detail they covered the following aspects:

Real Sharing Behaviour

Questions about sharing behaviour had the direction of “*What are the data storing and processing procedures of individuals?*” and “*Are employees aware of what data they share with whom?*”. They are based on Buchanan et. al (2007) who proved a relation between privacy concerns and technical protection users to protect their privacy. We slightly changed and included the questions asking for technical protection users take and included them in our questionnaire.

Trust in other users

The aim was to learn about “*Which data are employees willing to share, and with whom?*” and “*What influences the sharing behaviour?*”. We therefore took questions based on Malhotra et. al. (2004) who conducted a questionnaire focussing on the influence of trusting beliefs. Questions were changed to focus on colleagues.

Trust In Organisation

To get insights in questions like “*How do the trust in the organisation influence the sharing behaviour?*” and “*How common is sharing of data within the organisation?*” we worked with questions based on Schoorman et. al. (2007) which focus on organisational trust.

Individual privacy concerns

To measure the individual privacy concerns, that is how aware are individuals for possible problems based on personal information they disclose and we wanted to know “*How important are privacy and informational self-determination to employees?*”. Therefore we included questions from Smith et. al. (1996) which introduced a scale for privacy concerns used widely used also by the aforementioned authors.

In addition we, to be able to analyse the data statistically, we formulated five hypotheses to be answered by the survey:

- a) *Individual concerns about privacy is not directly related to real sharing behaviour.*
As described above we assume that there is a difference between how people describe their privacy awareness and concerns when asked for it directly and the way they handle this questions in real world situations. Privacy concerns in general might

⁹The privacy Questionnaire is included in the appendix of this document.

for example be influenced by reports in media about companies controlling their staff by video-surveillance.

b) *Sharing behaviour is related to trust in colleagues*

We assume that trust is crucial for something like collaborative reflection and data sharing. Therefore our hypothesis is that the more an individual trusts colleagues, the more personal information is already shared with them.

c) *Sharing behaviour is related to trust in the organisation*

As a second trust factor that comes into play especially when personal information is shared in computer systems can be found in trust in the organisation, as the organisation is mostly responsible for running these systems.

d) *Trust in colleagues is related to willingness to share data with them*

To take a more prospective look at the testbeds regarding sharing personal information for reflection support, we assume that there is a relation between how much trust exists towards colleagues and the willingness to share information with them under different circumstances.

e) *Trust in organisation is related to willingness to share data with the organisation*

As for question c) we also want to take into account possible relations between the willingness to share information with the employing organisation and the trust the individual has in the organisation.

Chapter 6 covers an in depth analysis of the hypotheses based on the questionnaire conducted in MIRROR testbeds.

4 Testbeds and sample

To get a broad overview of privacy and trust perception as well as data sharing behaviour, user studies for WP9 were conducted in all testbeds by use of a questionnaire included in the staff survey of KMRC. See Table 2 Testbeds and sample for privacy questionnaire Table 2 for an overview of testbeds and samples for the questionnaire.

Table 2 Testbeds and sample for privacy questionnaire

Testbed	Instrument	Partner	Application	Adaptations
RNHA	Privacy Questionnaire	KMRC/ RUB	Filled in by 71 employees of 2 different care homes	Special, shortened version for care homes
NBN	Privacy Questionnaire	KMRC/ RUB	Filled in by 39 employees of the stroke unit	
BT	Privacy Questionnaire	KMRC/ RUB	Filled in by 4 employees of the learning department	
Infoman	Privacy Questionnaire	KMRC/ RUB	Filled in by 3 sales consultants	
Regola	Privacy Questionnaire	KMRC/ RUB	Filled in by 17volunteers	

The sample of the WP 9 user studies includes all testbeds of MIRROR, as one of the aims of WP 9 is to derive insights and prerequisites for sharing information in order to inform application development in all testbeds. The size of samples in the respective testbeds, however, varies due to different sizes of the testbeds and different availability of staff to fill out questionnaires (see Table 2).

Due to the specific nature of the RNHA testbed - mainly a lower level of education and concern about the level of literacy - a shortened version of the staff survey with easier language was used. The modifications were well received by the testbed and likely lead to an increased response rate. While the level of detail and accuracy in which the key aspects can be captured is lower, these aspects can still be compared to the other testbeds.

4.1 Descriptions of the Testbeds

4.1.1 Registered Nursing Home Association (RNHA)

The **RNHA** testbed comprises a sample of Care Homes in the UK. The relationship between carers and residents provides challenges particularly to inexperienced carers. From their perspective as expert practitioners, RNHA have identified a suite of business needs to help improve care. For example, the carer must actively take into account the unique history of the patient to adequately handle situations occurring in day-to-day interaction.

Goals for the work of MIRROR at care homes of RNHA can be seen in improving people in care homes to provide the best possible care, to support the emotional well-being of all people in care homes (workers, residents and managers/owners) as well as aspects of the financial return for care home management and owners.

Constraints include the limited spread of Information and Communication Technology (ICT) within care homes where there is a culture of face-to-face communications; and multi-tasking managers with little senior support or time to network with others, and the fact that each care home is different.

4.1.2 Neurologische Klinik Bad Neustadt (NBN)

The **NBN** testbed consists of the medical staff in the stroke unit of the Neurological Clinic in Bad Neustadt, which can be divided into the professional groups of physicians, nurses and therapists. A big issue for care professions lies in coping with the amount of workload and emotional stress, although this is mostly neglected by hospitals. A key to preventing burn-out syndromes or similar problems lies in turning demanding situations into learning experiences by reflection on what was going on, how staff reacted to it, and if the reaction was beneficial in terms of outcomes.

Providing support for reflection based on experiences at NBN aims at tackling problems that arise from deficiencies in the individual's coping strategies for different forms of stress and, concerning collaborative reflection, at creating insights needed for continuously improving skills, work organisation, education training, continuing education and the like. By enabling support that facilitates reflection under time pressure, we can create a learning rich environment that is not only focused on factual knowledge or processes, but also on the tacit dimension of knowledge and the affective dimension. On the one side, this will clearly improve care/medical practices, but also safeguard the health of nurses and thus enable sustainable engagement. For the hospital as a whole, the service quality will be improved, and costs of absence will be reduced.

4.1.3 INFOMAN AG

The **Infoman** testbed consists of the staff of the Infoman headquarters in Stuttgart. The targeted end users of MIRROR are sales people. Currently systematic knowledge sharing and collaborative learning between sales consultants at Infoman happens only sporadically or directly based on personal relationships. Infoman offers a large number of technical possibilities for knowledge sharing. However, the necessary overview about all available resources are missing.

Infoman envisions their sales people and especially trainees to follow the innovative approach of MIRROR and to use the MIRROR prototypes. The sales people will be supported within their creative work to learn from previous sales experience in the organisation and transform the business and technical demands into offers for efficient processes and solid IT solutions.

The main strategic objective of Infoman AG is to analyse and optimise the marketing, sales and service processes of companies mainly active in the mechanical engineering industry. Infoman's sales people need to have a deep understanding of existing solutions and *broad knowledge of market demands*. In order to stay ahead of the competition and to best advise the customers each sales representative needs to continuously improve her skills in the focus field, rapidly learn aspects of other fields relevant to one customer project, and apply both within the customer's solution space. The uniqueness of each project as well as the time constraints in the offering process poses an essential challenge to Infoman.

4.1.4 REGOLA

The **Regola** testbed was run at the Civil Protection Organisation in Turin (Torino) and, when feasible, at the Regola headquarters. The Civil Protection in Turin is responsible for

coordinating the effort of personnel from several organisations with respect to disaster management in the Turin area and in collaboration with other Civil Protection units. This includes four different types of activities: Expectation, prevention, rescue and clearing emergency. Also, it involves three different levels: A ('ordinary events') B ('intermediate events') and C ('extraordinary event'). The operational structure includes many different organisations as well as a group of volunteers working directly for the municipality. Altogether there are about 450 volunteers coordinated by the Civil Protection in Turin.

The Civil Protection is stressing that simple and flexible resources are needed to handle events: emergency planning cannot be detailed and strict. It is difficult to organize training because of the discontinuous nature of the work. Some reflection and training (e.g. field trials) is happening within the associated organisations. A major challenge for the Civil Protection is to achieve learning from their experiences of handling the cases of disaster prevention and management. This involves volunteers learning from their own experience as well as that of others, across events, and also identifying individuals who might not fit as volunteers in crisis situations. A goal of introducing MIRROR solutions is to help the Civil Protection improve learning from experience among their volunteers on an individual, team and organisational level.

4.1.5 BT

The BT testbed is a branch of BT in the UK (BT Learning Solutions). Later on it is planned to expand the testbed to contract teams which manage the 1500 contracts BT has. A contract team consist of multiple members with responsibilities for the different areas of the contract like Sales, Delivery, service, etc. Each contract (team) is managed by a contract manager or contract director. Team members are engaged into a contract on a project basis. Therefore the team constellation changes from project to project. Team members also learn and share knowledge with their professional community (peers) and their contract teams. BT would like to investigate and test how MIRROR can contribute to more effective contract management processes by supporting effective working and learning practices for service technicians and contract teams.

In general, only applications which are very easy to use will be accepted. The team members have full schedules so it has to be clear what is in it for them. BT has a strictly managed IT infrastructure and strict rules on information management and where and how information is maintained etc. These will be difficult circumstances in which to implement MIRROR solutions.

5 Methods and research instruments

The questions in the privacy survey were organized in categories¹⁰ in line with the four aspects described in section 2.1. To broaden the view of *sharing behaviour* not only to the way sharing is done currently we focused some questions on how participants prospect their sharing behaviour in different circumstances:

- **Sharing behaviour (Q1.1-Q1.5):** We wanted to know how data sharing is handled at the moment with regard to personal information. This includes current practices of data protection such as shredding personal notes and asking for privacy statements from the employee.
- **Attitude towards sharing of personal notes (Q1.6-Q1.9):** For the purpose of MIRROR we wanted to know if there is a willingness to share personal documentation under different circumstances. Since there were not yet any MIRROR capturing apps to refer to we asked for sharing of notes as an easy to understand example.
- **Trust in colleagues (Q2.1-Q2.6):** These questions aim at the trust climate in the testbeds. We asked for the perception of the colleagues with regard to trustworthiness, predictability and assumed goals of the team in which the participants work.
- **Trust in the organisation (Q3.1-Q3.5):** Our hypothesis is that employees have different trust perceptions towards the organisation or a supervisor than towards colleagues. These questions ask how trustworthy they think their organisation is with regard to personal information and if they speak freely about their mistakes.
- **General privacy concerns (Q4.1-Q4.7):** Based on questionnaires from e-commerce contexts these questions cover concerns of individuals when asked for personal information in different situations.

In several questions we referred to terms like ‘personal information’, ‘team’ or ‘colleagues’, knowing that these terms can be interpreted differently depending on the situation or organisation the participant is working in. For example, at Regola the questionnaire was addressed to volunteers in a civil protection unit, at BT and Infoman “teams” are flexibly organized around projects and at NBN or RNHA participants work most of the time on the same ward or on a shift with the same colleagues. Nevertheless, we think there are similarities in perception of trust and data sharing between these groups regardless of the definition of these terms in detail. To create a simple common understanding the questionnaire began with a short introduction about our own understanding where we stated the following:

- **“Personal Information** refers to any information that relates to you as an individual. This includes your name or age, other personal data, but also data related to your work practice e.g., data logged in an attendance clock.
- **Team** refers to your colleagues with whom you work closely, e.g., in a project team, working unit or department.
- **Organisation** refers to the management of your organisation, i.e. your line manager and/or the general management.”

10 See the appendix of this document for the whole questionnaire.

In alignment with all other questionnaires which were part of the staff survey participants answered questions on a 5-point Likert-scale ranging from “strongly disagree” (1 point) to “strongly agree” (5 points).

Another difficulty was the different languages spoken in testbeds. While the original questionnaire was designed in English, which is suitable for RNHA and BT, we needed German translations for NBN and Infoman and an Italian version for Regola. Translation is always imprecise due to the inherent ambiguity of language. We addressed this problem by translating the questionnaire into English ourselves to ensure our intended implications were not distorted and we relied on Regola for translation into Italian.

6 Data analysis and results

The privacy questionnaire, as part of the staff survey, was completed by 133 participants. As can be seen in Table 2 there was a huge variation in returns from the different testbeds. This is related to the fact that especially at Infoman and BT the target group is considerably smaller than at NBN or RNHA. Staff in two different RNHA care homes volunteered to complete the survey which also helped to extend the number of participants in this testbed.

For a statistical analysis this makes it hard to compare results between different testbeds, as prerequisites for significance are only given in 2 testbeds. . And although we included all data into the analysis and found no significant differences between testbeds, the results cannot be generalized for BT, Infoman and Regola. On the other hand for the target group of sales consultants at Infoman it is to say that with three returns half of the sales consultants group participated. Where there were pronounced differences between the testbeds from a statistical view they are noted below and at some points we tried to enrich the analysis with examples from interviews and observations carried out in user studies of other WPs

The figures presented in the following analysis each cover groups of questions with a similar focus. The x-axis shows the number of the question and the y-axis shows the average of all answers to each question, where 5 means “strongly agree” and 1 “strongly disagree”. Within each bar lines indicate the standard deviation and numbers the number of respondents to the question. In addition some questions have an inverted scale e.g. participants were asked if they do not trust someone instead of if they trust. These inverted scales are visualized by a darker grey shading.

6.1 Analysis of descriptive statics

As described in chapter 3 the questions were from the outset categorized into five sections. The following analysis is structured by these sections to elaborate on the different categories and the findings.

6.1.1 Sharing behaviour

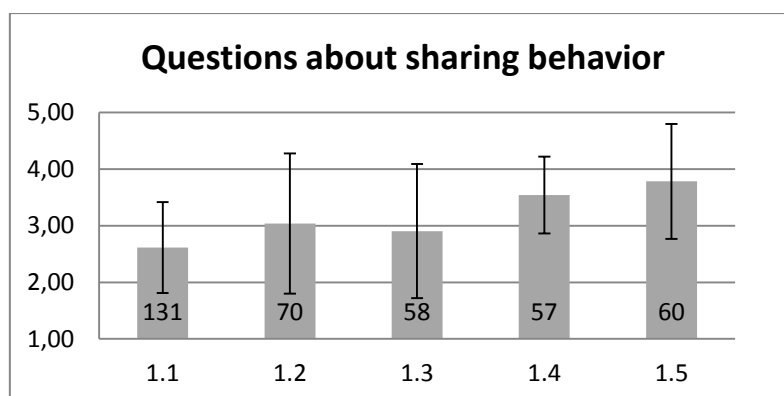


Figure 4: Averages of answers to questions about trust in colleagues; 5 = strongly agree; 1 = strongly disagree.

The first questions asked about **sharing behaviour**, where we wanted to know how participants behave in their organisation with regard to their personal information. Question 1.1 asked if participants “*talk to [...] colleagues about personal things or [...] feelings*”, with an average of 2.61. This is supported by the similar question 1.5 (“*In general, I hide personal information from others.*”). For questions 1.2 and 1.3 which asks for awareness about what others might do with their information (“*I always wonder what happens with my personal*

information when my employer or a colleague asks for it.” And “I inform myself about what happens with my personal information.”) average is 3.04 and 2.90 but with high standard deviations of 1.24 and 1.18, which shows that this is handled differently by individuals. Question 1.4 in addition asked for example behaviour (“I shred personal documents and notes at work or secure-delete digital information by overwriting the digital files when I don’t need them anymore.”) where the average is 3.5.

These questions show that it is not very common to share personal information in the testbeds, even 15% of the participants “strongly agree” to hiding personal information and one third do not regularly (answered with 1 or 2) talk about personal things. In addition there is a high deviation in awareness on how others might use personal information. Since MIRROR apps need voluntary participation of users when personal information come into play, information sharing needs to be fostered and data processing has to be transparent to encourage users.

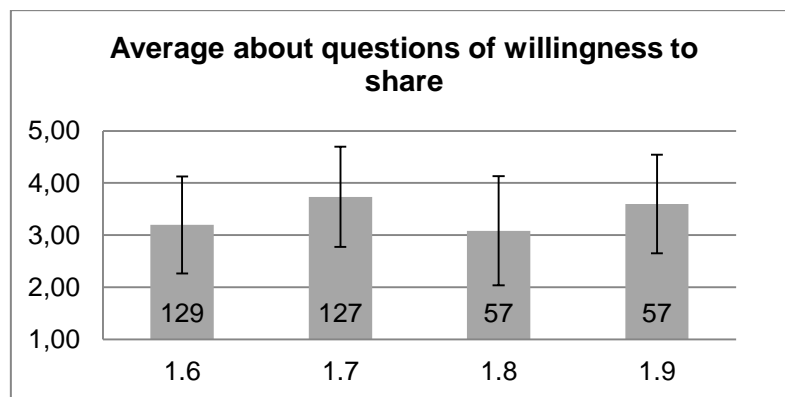


Figure 5: Averages of answers to questions about willingness to share. 5 = strongly agree; 1 = strongly disagree.

Figure 5: Averages of answers to questions about willingness to share. 5 = strongly agree; 1 = strongly disagree. shows the averages of answers to questions about **willingness to share** personal notes under specific circumstances. We see that there is a no refusal against sharing notes and personal information. A maximum of 6.64 % of participants strongly disagreed with the statements. The questions with slightly higher averages (1.7 and 1.9) implied more intrinsic motivation (“[...], if I know it would help them”) and support for sharing the right date (“[...] if I could easily make sure that they only have access to parts relevant for them.”). The other questions used conditions based on the behaviour of others (“[...] if my colleagues (1.6)/boss (1.9) would also do that”).

Although there seems to be no rejection of MIRRORs idea of sharing experiences and thus personal information there is on the other hand no enthusiasm to do so. Therefore it seems essential to make benefits visible for users and support users in sharing of information for specific purposes.

6.1.2 Trust in colleagues

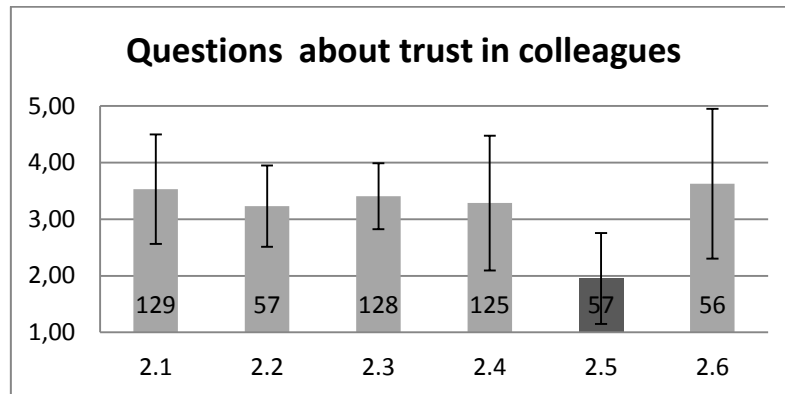


Figure 6: Averages of answers to questions about trust in colleagues. 5 = strongly agree; 1 = strongly disagree.

Questions 2.1 to 2.6 focussed on the perception of **trustworthiness of team colleagues**. From Figure 6 we see from 2.1 and 2.4 that there is at least a neutral (~ 40% answered with 3) or positive (~ 40% answered with 4 or 5) basis of trust. While questions 2.1 to 2.4 asked for personal appraisals for the trustworthiness and predictability of colleagues with regard to personal information provided by the participant (2.1 “*My team colleagues are trustworthy[...]*”, 2.4 “*My team colleagues are [...] predictable[...]*”) question 2.5 had an inverse scale asking for perception of dishonesty. The low average value at 2.5 supports the positive trust perception of the first questions. Question 2.6 asked for awareness of this trust relation when sharing personal information (“*When I decide to share personal data about my job with others, it always thoroughly think over whether I have built a relation of trust with them or not.*”). The high standard deviation (1.32) shows that there are large differences in practices here.

When we assume that trust between colleagues influences the way of personal information are shared and therefore influence how the MIRROR apps are used these results are not poor but also not very promising. If there is a relationship between sharing and trust, also trust has to be fostered by MIRROR apps. In addition the large differences between the awareness for trustworthiness of colleagues in context of sharing (2.6) indicate a need for differentiated modes of adjustability within MIRROR apps.

6.1.3 Trust in organisation

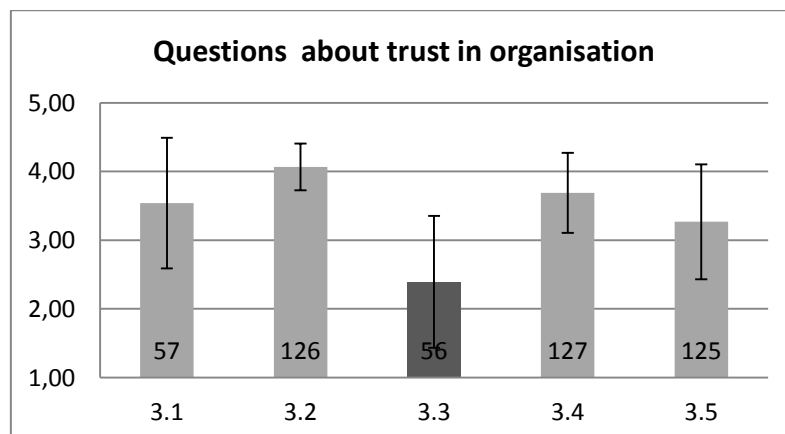


Figure 7 Averages of answers to questions about trust in colleagues. 5 = strongly agree; 1 = strongly disagree.

The block of questions from 3.1 to 3.5 deals with trust in supervisors and the organisation as a whole with regard to their handling of personal information. In general in all testbeds seem to have a good climate of trust between employees and employers. The high average of 4.06 to question 3.2 “*If my supervisor asked why a problem occurred, I would speak freely even if I were partly to blame.*” is especially interesting. The average is above 4 and was chosen by nearly 60% of the participants. At Infoman all participants answered with 5 (strongly agree), this corresponds to the low average of 2.39 to question 3.3 (which can be regarded as inverse questions to 3.2 “*Increasing my vulnerability to criticism by my supervisor would be a mistake.*”). The last two questions are focused on trustworthiness with regard to handling personal information (3.4 with average of 3.69) and the perception of organisations long-term view on employees’ morale (3.5 with average of 3.27). For both questions about 50% answered 4 on the scale.

As organisations later will operate the MIRROR apps and therefore have access to the central services they may be offered it is important that using the apps does not fail because of distrust in the operator.

6.1.4 General privacy concerns

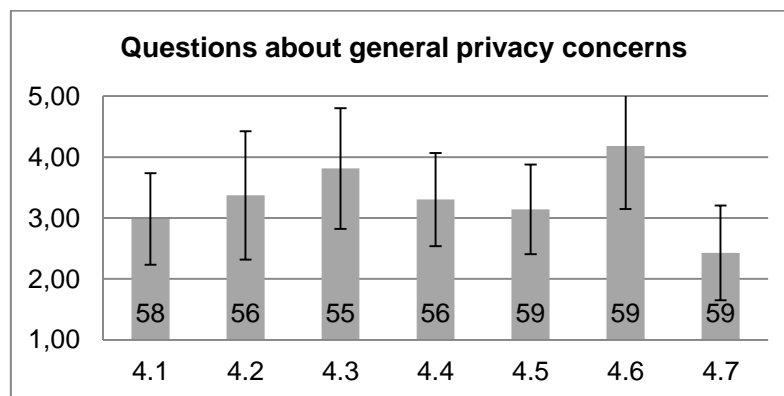


Figure 8: Averages of answers to questions about general privacy concerns. 5 = strongly agree; 1 = strongly disagree.

The questions about general **privacy concerns** ask participants about their attitude towards data collections, errors, secondary usage and improper access to databases of employees. The average of these concerns was between 3 and 4. We regard those who responded that way as *privacy pragmatists*, which means participants know about possible problems but that does not inhibit them from giving data to their employers. As can be seen from Figure 8, the averages for question 4.3 and 4.6 for all testbeds - except RNHA where these questions were not asked - are higher than for the other questions of this aspect. These questions both belong to the category “*unauthorized secondary use*” which state that employers have to take care that data about employees is only used for the purposes they were collected for. For question 4.6 46% of the participants answered with “strongly agree”. Question 4.7 (“*I’m concerned that my employer is collecting too much personal information about me.*”) where the average is below 3 shows that at the moment of answering the questionnaire participants were not concerned about excessive data collection by the employers.

In a comparison between testbeds it becomes apparent that the average answers for all but one question in this category are highest at NBN. This corresponds to reports from other

WP's stating that there is high privacy concerns at NBN which arises from awareness of privacy problems with regard to patient data.

For MIRROR especially the high rejection of secondary use of data is relevant. It has to be made sure organisationally and technically that employers are not able to use data from MIRROR apps for any other purpose than those participants consented in. In cases where a change of usage purpose is planned, users should be asked for new consent.

6.2 Analysis of correlations

Exploratorily, we looked for meaningful correlations in the data to get a first impression about those aspects of privacy that are related to each other. Pearson product-moment correlation coefficients (Pallant, 2007) showed that:

- Each questions 1.6 to 1.9 (*"I would share.."*) and 2.1 (*"I am completely convinced that my team colleagues are trustworthy in handling personal information about me."*) correlate positively with each ($r \sim .3$; $p < .03$; $n=56$). This indicates a positive **relation between perceived trust towards colleagues and the willingness to share.**
- Question 1.7 (*"I would share my notes and other personal information with my colleagues if I knew it would help them."*) correlates for all testbeds positive with question 3.4 (*"My organization is trustworthy in handling information about me"*). This indicates that **the more a participant trusts her organization, the more she is willing to share personal information with colleagues if it helps these colleagues.**
- Question 1.8 and 1.9 (*"I would share data [...], if my boss would also"* and *"I could make sure they get only relevant parts."*) correlate negatively with 3.4 (*"My organization is trustworthy"*) for all testbeds except RNHA. This can be interpreted as a support of the relevance of trust in the organization, as the more people are influenced by sharing supervisors or want more control over their data the less they trust the organization.
- For NBN 3.3 (*"Increasing my vulnerability to criticism by my supervisor would be a mistake."*) correlates positively with 1.9 (*"I would share my notes and other personal information with colleagues if I could easily make sure that they only have access to parts relevant for them."*). Although the questions address different sharing situations, one with colleagues and the other with a supervisor, the correlation indicates a need for enhanced control mechanisms when sharing personal information in cases where there is fear of negative effects of criticism.

We also looked for correlations between categories of items (in all testbeds but RNHA). While the data quality is limited and the results have to be taken with care, the following correlations seem relevant for our work:

- *Willingness to share* and *trust in colleagues* are related positively ($r=.364$, $p=.006$, $n=56$). **The more a participant trusts colleagues, the more she is willing to share personal information with them.**
- *Trust in colleagues* and *trust in organization* correlate positively ($r=.32$; $p=.014$; $n=58$). **We assume that little trust in colleagues also leads to little trust in the organization.**
- At least there is a positive correlation between *trust in organization* and *general concerns* ($r=.29$; $p=.027$; $n=58$). This correlation is not intuitive but might indicate that **the more participants trust their organization and supervisors the more they are**

aware of the fact that it could also be different and therefore are more concerned about their trust being abused.

In addition to correlation analysis between questions in the privacy questionnaire we compared answers with those from other parts of the survey.

- The correlation is positive between the overall scale from the privacy questions and years in team at RNHA, for other testbeds the ten questions were not sufficiently statistically reliable to be compared with other questions. This indicates that trust evolves over time and is dependent on the years one spends in a team to build up trust relations.
- For all participating testbeds we found that the scale from all privacy questions and the reflection questions as a whole correlate positively. This indicates that the more employees are in a trustworthy environment where personal information is shared the more they are willing to reflect. To those collaborative reflection seems fruitful and the willingness to participate is higher. This workplace correlation is strongest at NBN and least strong for Regola.

With regard to the hypotheses stated in section 3 we can say:

a) Individual concerns about privacy is not directly related to real sharing behaviour

We found no direct relations between the measured privacy concerns and the way people share personal data that can be generalized. Results from one testbed indicate that there might be a correlation between sharing and the concerns about on aspect of privacy concerns, unauthorized secondary use of the data, but this has to be further investigated to be verified.

b) Sharing behaviour is related to trust in colleagues

We could not generally approve this relation but found a correlation at NBN between answers to the questions “I talk to my colleagues about personal things” and “I fully trust my colleagues [...]” which could not be confirmed by data from the other testbeds. This indicates a relation which has to be taken into account.

c) Sharing behaviour is related to trust in the organisation

We found no correlation in for this in our dataset. This may be related to our questionnaire which asked about sharing with colleagues, and not explicitly sharing with the organisation. An interpretative explanation is that in working environments staff thinks about sharing with colleagues where effects are more direct visible and not about the organisation because of system complexity.

d) Trust in colleagues is related to willingness to share data with them

As described above there is a relation between trust in colleagues and the willingness to share personal data, at least for the testbeds where the full-length questionnaire was conducted. This implicates for MIRROR that we have to take trust relationships into account. For RNHA we also observed this behaviour as a participant stated in an interview that she was especially talking to those colleagues about problems that occurred during her work that she thought were more trustworthy.

e) Trust in organisation is related to willingness to share data with the organisation

This relation is indicated by the data of all but RNHA. Together with the strong refusal of secondary use of data for other purposes and dependent on the trust in the

organisation, this implies a greater need for security mechanisms to prevent misuse by the organisations and MIRROR apps.

Interpretation

The questionnaire responses confirmed the importance of trust as a prerequisite of sharing of personal information. We also were able to support three of our five hypotheses stating relations between aspects of privacy and trust derived from theory. For the testbeds we can say that there is a good trust in organisations with regard to data handling (Q3.4 >50% agreed) but also a strong refusal against secondary use of data that was not intended when data was captured in the first place (nearly 50% strongly agreed 5). This point is important because trust in organisation also correlates with willingness to share with colleagues, which we want to foster. Therefore MIRROR apps need user centred adjustable controls for which data is shared with whom. Furthermore the willingness to share is not that high overall, but it is higher for goals related to helping colleagues particularly if they can only get access to data they need. This indicates a need for transparency about what data helps colleagues and transparent mechanisms to share only specified parts for a given purpose. In addition there is a high deviation between individual needs to inform oneself e.g. with company agreements and other transparency mechanisms about technical as well as organisational details about data processing within the apps which has to be taken into account within the development.

7 Overview and recommendations

7.1 Recommendations from user studies

The user studies conducted in WP9 revealed the complex relationships between privacy and trust as influential factors for data capturing and sharing. To make sure MIRROR applications are accepted in the testbeds and more widely we therefore have to take privacy and security mechanisms into account for further development.

In this deliverable we first described the requirement of privacy from different perspectives. We identified trust as the underlying mechanism that enables users to collaborate and share personal information without having to think about possible risks every time they talk to a colleague. Trust is therefore a relevant basis for fostering reflection on different levels. Individuals that want to reflect and use MIRROR apps have to trust these technical systems that they do not unintentionally share their data with third parties. They also have to trust their colleagues when making their reflection outcomes public to them as well as their supervisors when they want to change something after they have been involved in a situation where something went wrong. Sharing of reflection outcomes as well as data captured about individuals or groups require trust in colleagues and the organisation. This enables reflection participants to be sure data is used for their own and the groups advantage instead of being concerned about possible disadvantages. The need for mechanisms that support this belief is even more important when it comes to organisational reflection for which participants have to give access to their captured data on an aggregated or anonymous basis.

For authorization and privacy enhancing technologies technical means exist or are currently developed in other EU funded projects like Tas³ or PrimeLife. We described some mechanisms in this deliverable and decisions are to be made which mechanism fits all privacy needs within the MIRROR appsphere with regard to the legal baseline which was also described. As a result from the user studies and its analysis (cf. section 6) we would stress three main topics that have to be taken into account:

1. Since there is a strong refusal of secondary usage of data although participants trust their organisation we see a need to enforce data security mechanisms especially **confidentiality** to ensure MIRROR app users are in control of who has access to their data.
2. The very individual view on privacy and concerns about it can be seen as a need for **transparency** with respect to which data is available as well as what happens with it. This would not only to support users in their rights to be in control and therefore gain trust, but would also foster awareness about when the data they share helps others and keep track about how reflection outcomes are implemented in their work practice. Transparency mechanisms can also support building of trust relations especially towards the organisation since it is comprehensible for users how their personal information is used.
3. Since some users have higher personal standards and privacy concerns than others independent from the testbed they are working in we recommend mechanisms of **adjustability** to allow individual settings according to user needs. Also trust is a flexible and changes over time. Therefore models for Access Control Policies (ACP) have to be developed that on the one hand fit users' needs and on the other are easy to use.

8 Appendix A: Guidelines for Actions to Safeguarding the Abuse of Personal Data Collected with Mirror Apps

8.1 Data classification

The data to be collected during the user studies should be categorized as follows:

- a) data that do not qualify as personal data (e.g., information about the organisation, the location or the size of the company)
- b) anonymous personal data (see Pfitzmann and Hansen, 2010)
- c) coded/pseudonymised personal data
- d) non-coded personal data (a single person is identifiable e.g., by name or by her position in an organisation where only one person has this position)
- e) secondary non-coded personal data
- f) organisation-specific coded data (i.e. the organisation's name is a pseudonym)
- g) organisation-specific non-coded data (i.e. it is clear which organisation is meant)

8.2 Overview of the actions by type of data

Table 3 gives an overview of actions to be taken for a specific category of data

Table 3: Overview of types of data for and actions to be taken.

Action	Non Personal Data	Anonym. Personal Data	Coded Personal Data	Non coded Personal Data	Secondary non coded Personal Data	Organisati on Specific Coded Data	Organisatio n Specific Non-coded Data
Non disclosure agreement	No	No	Yes	Yes	Yes	Yes	Yes
Inform the organisation about data policies	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inform data subject about data policies	No	No	Yes	Yes	Yes, if possible	Yes	Yes
Get consent from organisation	No	No	Yes	Yes	Yes, if possible	Yes	Yes
Get consent from data subject (individual)	No	No	Yes	Yes	Yes, if possible	No	No
Implement secured data access for data subjects	No	No	No?	Yes	No	No	No
Define maximum data retention policy	No	No	Yes	Yes	Yes	Yes	Yes
Define review process	No	No	Yes	Yes	Yes	Yes	Yes

8.2.1 Non disclosure agreement

Document a non-disclosure agreement for all individuals involved in the collection, analysis and reporting of personal data collected with the MIRROR apps, and ensures that they all have signed this non-disclosure agreement.

Document the penalties that will apply in the event of a breach of the non-disclosure agreement, and how the organisations and data subjects that are involved will be informed in this event.

Specify the code of conduct as part of the non-disclosure agreement.

8.2.2 Inform the organisation about data policies and get consent

- Inform the management of the organisation using MIRROR apps about:
 - The objective of MIRROR;
 - The methods of data collection;
 - The types of data collected;
 - The actual process for safeguarding the privacy of the data subject and the organisation;
- Check whether specific provisions are made within the organisation relating to safeguarding personal data
- Check whether specific organisation bodies (e.g. workers' council, data protection officer) have to be informed / give consent to the user studies and related collection of personal data

8.2.3 Inform data subjects about data policies

- Inform the data subjects (individuals) about the of MIRROR apps;
- Inform the data subject about the types of data collected and how their privacy will be safeguarded
- Inform the data subjects how they will be involved in the verification and approval of the collected data
- Inform the data subjects how they can get access to their archived personal data once the data is stored
- Inform the data subjects how the collected data will be used and reported on.

8.2.4 Get consent from the organisation

- Obtain written consent from an authorized representative of the organisation as well as specific organisation bodies (e.g. workers' council, data protection officer) for the proposed collection, storage, analysis and reporting of personal data and organisational data collected in their organisation.

8.2.5 Get consent from the data subject (individual)

- Obtain written consent from the data subject for the proposed collection, storage, analysis and reporting of their personal data collected.

8.2.6 Implement secured data access for data subjects

- All personal data stored about a data subject should be accessible (through secured data access) for the data subject or his/her authorized representative. It should be clear to the data subject, where his/her personal data is stored and how to get access. This can be mentioned before the data is collected together with getting the consent. People only have to get access to data that can be traced back to their identity. So this means only for non-coded personal data. So this is not needed for anonymised or coded data.
- The data subject must be informed how (and where) the personal data stored after the data collection can be accessed by the data subject.
- Only the data related to that individual data subject should be accessible.
- Instructions should be made available to the data subject, describing what to do if anomalies are found.
- The data subject should be informed about the retention period for the personal data stored.

8.2.7 Define maximum data retention and disposal policy

- The maximum retention period for non-coded personal data should be identified and communicated to all involved parties.
- There should be procedures implemented to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques

8.2.8 Define review process

- A procedure to verify that all arrangements to prevent unintended abuse of personal data that could breach the privacy of data subjects should be in place.

9 Appendix B: Privacy Questionnaire

Of special interest for: **WP9**

Purpose: The purpose of the Privacy Questionnaire is to assess the stance of the testbed employees regarding privacy - which includes sharing of information, trust in team members, trust in management staff, and concern with regard to the handling of personal data by the organization.

Research Questions to be answered:

- What is the level of privacy concern for different individuals?
- How comfortable are the users with these policies?
- What influences the sharing behaviour (e.g., hierarchy, structure, personal relations)?
- How do the different types of trust influence the sharing behaviour?

Target Group: End-Users of the MIRROR-Apps

Description: The questionnaire will shed light on the four separate issues of General Privacy Concern vs. Real Sharing Behavior as well as Trust in Management and Trust in Colleagues. Trust is the key issue that impacts the willingness to share personal information. The questionnaire will be applied within all testbeds either paper-based or as a web-based questionnaire. *Important Note -- Reversed Items:* Some items are inverse scaled and must be reversed for analysis!



In this questionnaire, we would like to ask you about your attitudes to privacy. Kindly answer the following questions as they apply to you.

- „Personal Information“ refers to any information that relates to you as an individual. This includes your name or age, other personal data, but also data related to your work practice e.g., data logged in an attendance clock.
- „Team“ refers to your colleagues with whom you work closely, e.g., in a project team, working unit or department.
- „Organisation“ refers to the management of your organisation, i.e. your line manager and/or the general management.

Please indicate your agreement with the following statements.		strongly disagree	disagree	neutral	agree	strongly agree
(1.1)	I regularly talk to my colleagues about personal things or my feelings.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.2)	I always wonder what happens with my personal information when my employer or a colleague asks for it.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.3)	I inform myself about what happens with my personal information in computer systems at work before using them (e.g. by reading company agreements negotiated between the works council and management)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.4)	I shred personal documents and notes at work or secure-delete digital information by overwriting the digital files when I don't need them anymore.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.5)	In general, I hide personal information from others.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.6)	I would share my notes and other personal information with my colleagues if they would also do that.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.7)	I would share my notes and other personal information with my colleagues if I knew it would help them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.8)	I would share my notes and other personal information with my colleagues if my boss would also share his personal information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(1.9)	I would share my notes and other personal information with colleagues if I could easily make sure that they only have access to those parts that are relevant to them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2.1)	My team colleagues are trustworthy, as far as handling personal information about me is concerned.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2.2)	My team colleagues never tell the truth or fulfil promises related to information provided by me.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2.3)	I trust that my team colleagues would keep my best interests in mind when dealing with information about me and my work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

(2.4)	My team colleagues are in general predictable and consistent regarding the usage of information about me and my work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2.5)	My team colleagues are never honest with me when it comes to using information about me and my work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2.6)	When I decide to share personal data about my job with others, it always thoroughly think over whether I have built a relation of trust with them or not.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3.1)	My superior keeps my interests in mind when taking decisions that affect me and my work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3.2)	If my superior asked why a problem occurred, I would speak freely even if I were partly to blame.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3.3)	Increasing my vulnerability to criticism by my superior would be a mistake.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3.4)	My organisation is trustworthy in handling personal information about me.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3.5)	My organisation considers the impact of decisions on employee morale.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.1)	It usually bothers me when I am asked to supply personal information about me at work.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.2)	Any personal information in computer databases at work should be double-checked for accuracy — no matter how much this costs.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.3)	Employers should not use personal information for any purpose, unless it has been authorized by the individuals who provided the information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.4)	Employers should devote more time and effort to prevent unauthorized access to personal information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.5)	If my employer asked me to use a computer system in which I have to enter personal information, I would feel uncomfortable about that.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.6)	When people give personal information to an employer for some reason, the employer should never use the information for any other reason.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4.7)	I am concerned that my employer is collecting too much personal information about me.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

References

1. Ardagna, C. A., S De Capitani di Vimercati, und P Samarati. 2006. Enhancing User Privacy Through Data Handling Policies. In Data and Applications Security XX, 4127/2006:224-236. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Juli 19.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.932&rep=rep1&type=pdf>
2. Bhatti, R., E. Bertino, und A. Ghafoor. 2005. A trust-based context-aware access control model for web-services. Distributed and Parallel Databases 18, no. 1: 83–105.
3. Buchanan, T., C. Paine, A. N Joinson, und U. D Reips. 2007. “Development of measures of online privacy concern and protection for use on the Internet.” Journal of the American Society for Information Science and Technology 58 (2): 157–165.
4. Dürbeck, Stefan, Jan Kolter, Günther Pernul, und Rolf Schillinger. 2010. Eine verteilte Autorisierungsinfrastruktur unter Berücksichtigung von Datenschutzaspekten. Informatik-Spektrum 33, no. 03/2010. doi:10.1007/s00287-009-0411-0.
<http://dx.doi.org/10.1007/s00287-009-0411-0>.
5. Dewan, Prasun, und Honghai Shen. 1998. Flexible meta access-control for collaborative applications. In Proceedings of the 1998 ACM conference on Computer supported cooperative work, 247-256. Seattle, Washington, United States: ACM. doi:10.1145/289444.289499.
<http://portal.acm.org/citation.cfm?id=289444.289499&type=series>.
6. Fischer-Hübner, Simone, Luigi Iacono, und Sebastian Möller. 2010. Usable Security und Privacy. Datenschutz und Datensicherheit - DuD 34, no. 11: 773-782. doi:10.1007/s11623-010-0210-4.
7. Geambasu, Roxana, Tadayoshi Kohno, A Levy, und HM Levy. 2009. Vanish: Increasing Data Privacy with Self-Destructing Data. In Proc. of the 18th USENIX Security Symposium. <http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.txt>.
8. Hansen, M. 2008. Study on protocols with respect to identity and. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.8_Study_on_protocols_with_respect_to_identity_and_identification.pdf.
9. Herrmann, T. 2001. „Kommunikation und Kooperation“. CSCW-Kompendium. Lehr- und Handbuch zum computerunterstützten kooperativen Arbeiten (S. 15-25). Berlin et al.: Springer.
10. Iachello, Giovanni, und Jason Hong. 2007. „End-user privacy in human-computer interaction“. Found. Trends Hum.-Comput. Interact. 1 (1): 1-137.
11. Kramer, R. M. 1999. „Trust and distrust in organisations: Emerging perspectives, enduring questions“. Annual review of psychology 50 (1): 569–598.
12. Langheinrich, Marc. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In Ubicomp 2001: Ubiquitous Computing, 2201/2001:273-291. Lecture Notes In Computer Science. Springer Berlin / Heidelberg.
http://dx.doi.org/10.1007/3-540-45427-6_23.
13. Malhotra, N. K, S. S Kim, und J. Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” Information Systems Research 15 (4): 336–355.
14. Nepal, Surya, John Zic, und Julian Jang. 2009. A Policy Based Approach to Managing Shared Data in Dynamic Collaborations. In On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, 1296-1303.
http://dx.doi.org/10.1007/978-3-540-76843-2_11.
15. Paar, Christof, und Jan Pelzl. 2009. Understanding Cryptography: A Textbook for Students and Practitioners. 1., st Edition. 2nd Printing ed. Springer, Berlin, December 10.

16. Pekárek, Martin. 2009. Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces. Juli.
<http://www.primelife.eu/results/documents>.
17. Pallant, J. (2007). SPSS Survival Manual. McGraw-Hill, Open University Press.
18. Perlman, Radia. 2005. The ephemerizer: making data disappear. Sun Microsystems, Inc. <http://portal.acm.org/citation.cfm?id=1698176>.
19. Rost, Martin, und Kirsten Bock. 2011. Privacy By Design und die Neuen Schutzziele. Datenschutz und Datensicherheit 35, no. 1: 30-35.
20. Schoorman, David, Roger Mayer, and James Davis. 2007. "An integrative model of organizational trust: Past, present, and future." *Academy of Management Review* 32 (2): 344-354.
21. Seifert, Matthias and Pawlowsky, Peter. 1998. „Innerbetriebliches Vertrauen als Verbreitungsgrenze atypischer Beschäftigungsformen“. *Mitteilungen aus der Arbeitsmarkt- und Berufsforschung* 31 (3): 599-311.
22. Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns about Organisational Practices." *MIS Quarterly* 20 (2) (June): 167-196.
23. Tolone, William, Gail-Joon Ahn, Tanusree Pai, and Seng-Phil Hong. 2005. Access control in collaborative systems. *ACM Comput. Surv.* 37, no. 1: 29-41.
doi:10.1145/1057977.1057979.
24. Westin, A. F. 2003. „Social and political dimensions of privacy“. *Journal of Social Issues* 59 (2): 431–453.
25. Whitten, A., und J. D Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In 8th USENIX Security Symposium. August.
26. Zhang, G., und M. Parashar. 2004. Context-aware dynamic access control for pervasive applications. In *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference*, 21–30.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.1258&rep=rep1&type=pdf>