From H1.3.5: Requirements and concepts for identity management throughout life

Editors:	Katalin Storf (ULD)
	Marit Hansen (ULD)
	Maren Raguse (ULD)
Reviewer:	Stuart Short (SAP)

Identifier:	H1.3.5
Type:	Heartbeat
Class:	Public
Date:	November 30, 2009

Abstract

This report derives requirements and concepts for identity management throughout life, taking into account lifelong aspects of privacy and identity management which demand for a new consideration of legal and technical protection. This Heartbeat is a draft document presenting the current state of discussion in Work Package 1.3. Basing on H1.3.2 (the draft version of H1.3.5), this Heartbeat presents a multitude of requirements which have been refined by taking into account all other reports that have been elaborated in this Work Package, yet. These requirements form a basis for the further work, in particular on prototype development in Work Package 1.3. In addition it addresses stakeholders such as system developers, application providers, and policy makers by pointing out important issues to consider when setting long-term conditions of societal living and technological support. This Heartbeat is made public to enable public review and to foster input from other actors.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe-Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

This deliverable has been jointly authored by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable.

Chapter	Author(s)
Executive Summary	Katalin Storf (ULD), Marit Hansen (ULD)
1 Introduction	Katalin Storf (ULD)
2 Fundamental definitions within privacy throughtout life	Katalin Storf (ULD), Marit Hansen (ULD), Andreas Pfitzmann (TUD), Sandra Steinbrecher (TUD)
3 High-level requirements for Privacy4Life and the Seven "Laws of Identity"	Katalin Storf, (ULD), Marit Hansen (ULD), Maren Raguse (ULD), Arnold Roosendaal (TILT), Ulrich Pinsdorf (EMIC)
4 Requirements concerning different actors	Katalin Storf (ULD), Marit Hansen (ULD), Maren Raguse (ULD), Arnold Roosendaal (TILT), Aleksandra Kuczerawy (K.U. Leuven), Karel Wounters (K.U. Leuven)
5 Tools and mechanisms for Privacy4Life	Sandra Steinbrecher (TUD), Andreas Pfitzmann (TUD), Rainer Böhme (TUD), Stefan Berthold (TUD), Marit Hansen (ULD)
6 Recommendations for policy makers	Marit Hansen (ULD), Katalin Storf (ULD)
7 Conclusion and outlook	Katalin Storf (ULD)

Table of Contents

List of Figures

Executive Summary

It is nothing new – and since a few years widely accepted by the majority of market players as well as governmental authorities – that privacy and identity management is necessary for our information society. While further constructing and building the technological skeleton of our society, it becomes clear that long-term aspects have mostly been neglected by now. The regulation of privacy and data protection does not cope with many evolving new technologies, and it does not seem to be effective when it comes to Web 2.0 applications which build on sharing pieces of (personal) data with big user groups. Moreover, technological concepts which provide long-term protection are missing. Additionally, identity-related applications in the governmental context seem to show deficiencies when it comes to the concept of "Privacy4Life", i.e., enabling and supporting people to maintain their privacy throughout their lives.

This Heartbeat H1.3.5 within the PrimeLife Work Package 1.3 "Managing identity, trust and privacy throughout life" documents the results of the analysis of common issues and requirements for privacy-enhancing identity management support throughout one's whole life. Since this is a very broad scope, this document derives requirements for developers and providers of applications, information and communication technologies (ICT) infrastructures, third parties which can support Privacy4Life, users or other data subjects. In addition it lists recommendations for policy makers (in particular law makers, standardisation bodies, and politicians).

The elobarated requirements are divided in high-level requirements and more fine-grained ones that address selected scenarios. In particular today's privacy principles from European law and the OECD as well as their current implementation in law and technology are investigated with respect to their long-term effects: transparency, data minimisation, fair use, and user control. This list is supplemented by requirements on the practicability of mechanisms and on the necessity of dealing with changes in society, law, and technology. When going into more detail, specific requirements address, among others, social network providers when designing their applications, conditions for delegation of privacy functionality in case the individual cannot manage her privacy on her own, or the area of digital heritage, i.e., how to express one's wishes for the time after one's death.

The analysis of technological primitives and tools that can be used to better support individuals in their life-long privacy and identity management shows the existence of a lot of interesting and potentially useful mechanisms. However, there seems to be a long way to go before a comprehensive solution can be offered to individuals. The recommendations to policy makers take that into account and propose that law makers and standardisation bodies should set the course clearly towards privacy and identity management throughout life.

Subsequent to this Heartbeat, Deliverable D1.3.1, "Scenario, Analysis and Design of PrivacyThroughout Life Demonstrator" will briefly outline the findings of H1.3.5 and concatenate them with the results of the analysis of privacy and identity management throughout life as well as the definition of the prototype.

Chapter 1

Introduction

The objective of the Heartbeat H1.3.5 is to derive common issues and requirements for privacy-enhancing identity management support in daily life throughout one's whole life and to develop concepts necessary for the implementation of these applications – in short: **Privacy4Life**. This Heartbeat is based on some PrimeLife deliverables.[1] Some requirements are acquired from PrimeLife Activity 5 to further extend the collaboration between the work packages.[2] The elaborated requirements will serve as the basis for developing and testing prototypes demonstrating the feasibility of enhancing identity management throughout one's whole life in a sustainable way. Thereby, this Heartbeat will bridge the more abstract work on analysis as performed in the foregoing deliverables[3] and the concrete work on prototypes.[4]

Working on the issue of Privacy4Life in PrimeLife, the project very much benefits from interdisciplinary discussions. These discussions will be continued in further work of Work Package 1.3. This Heartbeat reflects work in progress and therefore cannot offer a comprehensive, consistent and proven model for the Privacy4Life concept. However, within PrimeLife it will be possible to approach the issue from different angles and to sketch various ideas which help to support the Privacy4Life concept.

This Heartbeat tries to demonstrate workable requirements and concepts on selected scenarios and elaborates options for action by various stakeholders: policy makers (in particular law makers, standardisation bodies, and politicians), developers and providers of applications and ICT infrastructures, third parties which can support Privacy4Life, and users or other data subjects. Requirements, named in the deliverable may be defined as technical, legal or social.

The document is organised as follows: Chapter 2 outlines general definitions of data protection law and gives interpretations in the light of privacy throughout life. Especially current legal definitions are preceded and deficits in current legal definitions are revealed. These general

[1] H1.3.1: Draft of: Analysis of privacy and identity management throughout life; H1.3.3: Analysis of privacy and identity management throughout life; H1.3.2: Draft of: Requirements and concepts for privacy-enhancing daily life.

[2] D5.1.1: Requirements for next generation policies.

[3] H1.3.1, H1.3.2 and H1.3.3.

[4] H1.3.4.

definitions should guide through the document and are derived from the Data Protection Directive 95/46/EC [Euro95] and the ePrivacy Directive 2002/58/EC [Euro02] of the European Parliament as well as from some internal PrimeLife deliverables.[5] Chapter 3 in particular gives an overview of high-level requirements for Privacy4Life. Chapter 3 furthermore refers to Kim Cameron's Seven Laws of Identity [Came05] under the aspect of an individual's whole life and takes up the Laws of Identity to see to what extent they are applicable on the individual's life. Chapter 4 analyses in more details the requirements on the basis of the high-level requirements mentioned in chapter 3. Explicit requirements are derived for selected scenarios throughout life and referring to the individual's digital footprints. The term "digital footprint" refers to the definition in PrimeLife work package 1.[6] Digital footprint refers to the personal data that accumulates in information systems and is mostly unknown by the particular person. Making the digital footprint visible can be very helpful in rising awareness. These requirements address various stakeholders such as application providers and system developers. Chapter 5 summarises tools and mechanisms for Privacy4Life. Finally Chapter 6 gives detailed recommendations for policy makers to realise the requirements.

[5] H1.3.4, H1.3.2, H1.3.3 and H5.1.1.

[6] H1.3.4.

Chapter 2

Fundamental definitions within privacy throughout life

This chapter outlines fundamental definitions of data protection law and interprets it in the light of privacy throughout life. It especially defines the current legal definitions and furthermore shows deficits in current legal definitions. These definitions have general character and therefore are prepended as a general explanation.

2.1 General Definitions

Most of the common definitions are derived from the Data Protection Directive [Euro95], from the ePrivacy Directive [Euro02] as well as from previous PrimeLife heartbeats as follows:

Data subject

An identifiable natural person[7], which is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [Euro95, Art. 2a].

Data subject's consent

Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed [Euro95, Art. 2c].

Data controller

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by National or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law [Euro95, Art. 2d].

[7] We also use the term "individual" or "human being" for "natural person".

Processing (of personal data)

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. This also includes the action of anonymisation or pseudonymisation of personal data, even if after such action the data may no longer constitute personal data [Euro95, Art. 2b].

Privacy-relevant data processing

Not only processing of personal data may affect the privacy of an individual. For instance the provision of ICT systems which enable linkage of data can be relevant to the private sphere of the individual because this linkage may yield personal profiles on which decisions are based [HaMe07, LaRo08]. Similarly, ICT systems which aggregate data to group profiles instead of personal profiles may affect the private sphere of each individual concerned by enabling her discrimination [Phil04]. Further, not all parts of an ICT system that processes personal data touch those data themselves; still they can be relevant for the system's decision-making based on individuals. Note that with service-oriented architecture this phenomenon is by no means rare, but prompts questions to the responsibility for data protection of the data subjects concerned. The term "privacy-relevant data processing" encompasses all these ways of data processing.

Data processor

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller [Euro95, Art. 2e].

User

User means any natural person using a publicly available electronic communications service, without necessarily having subscribed to this service [Euro02, Art. 2a].

Developer of an ICT system (or system developer)

A natural or legal person that is involved in conceptualising, designing and/or implementing an ICT system. Taking a wide view on the term "system", "system developers" are meant to include "application designers".

Application provider (or service provider)

A natural or legal person that operates an application based on an ICT system and offers it to users.

Policy maker

A natural or legal person with power to influence or determine policies and practices at an international, national, regional, or local level. This comprises law makers, standardisation organisations for technical standards, and supervisory authorities. In addition privacy organisations which are not institutionalised by a State can play a role as well as media such as the press or bloggers – these can be considered influential to policies although the narrow term of "policy maker" usually does not comprise media.

Care-taker

A natural or legal person with some responsibility for an individual, for example, a parent, a teacher, a trainer or an employer. It is sufficient if the person feels the responsibility. In the area of privacy, a care-taker should try to empower others in self-determination.

Stage of life

A stage of life of an individual with respect to managing her privacy is a period of life in which her ability to do so remains between defined boundaries characterising this stage of life

[CHP+09]. Every individual during her lifetime passes through one or more stages during which she does not have the ability to understand the consequences of data processing relevant to her private sphere or to act upon that appropriately.

Delegation

Delegation is a process whereby a **proxy** (also called delegatee or agent) is authorised to act on behalf of a **principal** (also called delegator) via a mandate, i.e., transferred duties, rights and the required authority, from the principal to the proxy. The field of delegation has been discussed by various authors, mainly aiming at technical solutions for specific scenarios. Putting the focus on privacy aspects, we deviate a bit from the definitions used in [PRCD09] or [Cris98]. In our setting, both principal and proxy are natural persons.[8] The delegation may be invoked by the principal herself, but there are also cases where other entities explicitly decide on the delegation (for example, in the case of incapacitation of person the guardianship court) or where the delegation is foreseen in law (for example, when parents are the default proxies of their young children). The power of proxy is usually assigned for a specific period of time.

Data handling policies

Data handling policies were already defined within PrimeLife as a set of rules stating how a piece of personal data should be treated.[9]

2.2 Data types

During one's lifetime many different kinds of data appear and many different data may be disclosed by the data subject. This might be data about the data subject herself or data about others. The following data types can be defined:

Personal data

Any information related to an identified or identifiable natural person. Natural persons are only living individuals but neither deceased nor legal persons [Euro95, Art. 2a].

Note that [Arti07] refines this definition by elaborating on "any information", "relates to", "identified or identifiable" and "natural person". This work is quite helpful for practitioners; however, there are still open issues, in particular concerning new technologies and concerning intercultural settings where the terms may be interpreted differently, for example, pointed out in [LaRo08].

Special categories of data [Euro95, Art. 8]/"sensitive data"

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life (these categories of data are also referred to collectively as **"sensitive data"**).
- Personal data relating to offences, criminal convictions or security measures.
- National identification numbers or any other identifiers of general application.

Note that the sensitiveness of data perceived by an individual may be different from what is expressed by the special categories according to Art. 8 of the European Data Protection Directive

[8] It is also possible that legal persons become proxy, for example, organisations for children's welfare, public youth welfare office. And under certain circumstances even the principal may be a legal person. However, broadening the view to legal entities overstrains the scope of this text and may be a task for future research.

[9] See D5.1.1.

[Euro95, Art. 8]. Moreover, concerning long-term risks in an unpredictable setting, the view on the sensitivity of an individual's data should be broadened, as proposed in [CHP+09] based on [HaMe07]:

- **"Data may be static, or changes are quite accurately predictable:** Data which are static over time and are disclosed in different situations enable linkage of related data. Examples for static data are date and place of birth. Similar to static data are those which are quite accurately predictable or guessable because they follow some rules. […] If static identity information is being used for purposes such as authentication, this bears a risk because these data cannot easily be revoked and substituted […].
- **Data may be (initially) determined by others:** Data which the individual concerned cannot determine himself (for example, the first name) may persist or it may take a significant amount of time or great effort to change them. A special case is the inheritance of properties from others, for example, the DNA being inherited from the natural parents.
- **Change of data by oneself may be impossible or hard to achieve:** If data are static (see above) or if data are not under the individual's control, wilful changes may not be possible. Examples are data processed in an organisation.
- **Inclusion of non-detachable information:** Data that cannot be disclosed without simultaneously disclosing some side information tied to the data should be prevented or the individual should at least be made aware of this. Examples are simple sequence numbers for identity cards which often reveal sex, birth data and at least a rough timeframe of when the identity card was issued [HaMe07].
- **Singularising:** If data enable to recognise an individual within a larger group of individuals, the individual privacy may be invaded by tracking or locating, even if other personal data of the individual are kept private.
- **Prone to discrimination or social sorting:** There are no data which are definitely resistant against a possible discrimination forever. This does not need the individual to be identified or singularised. If some people disclose a property and others resist to do so, this already allows for social sorting or positive discrimination." [CHP+09]

Partial identities

Personal data can be represented by so-called **digital identities** consisting of attributes, i.e., sets of personal data. A **(digital) partial identity** is a subset of these attributes – depending on the situation and the context both in the physical and digital worlds – that represents an individual [PfHa08]. Note that a digital identity usually is only growing, never shrinking over time because it is very hard – if not impossible – to erase widely used digital data [HaPS08]. Consequently, it cannot be expected that privacy-related activities, such as disclosure of personal data, or their consequences are revocable.

2.3 Areas of life

Individuals interact with other individuals and organisations in many different relations, all of which are connected to different roles of the individual. **Identity** was already defined by Goffman as "the result of publicly validated performances, the sum of all roles played by the individual, rather than some innate quality" [Goff59].

The data set which characterises a role can be regarded as a **partial identity**. Depending on the context (relation) between the individual and the person or entity they interact with, certain information is disclosed or not. The information disclosed and characteristics associated to the individual are attributes of this individual. Individuals from a data perspective can therefore be

seen as a (large) collection of attributes. For a concrete partial identity the attributes take specific values. So ‘first name’ is an attribute label while ‘Peter’ is an attribute value.

In daily life, people are subject to various subscriptions and therefore have special behaviours and follow special rules depending on the contexts. They even want to present different faces of themselves, depending on the impression they want to conciliate. Therefore the data subject also distinguishes which audience is allowed to see which data of him/her. Audience segregation is a device for protecting fostered impressions. If everyone had access to all information related to an individual all the time, relationships would no longer be possible.

Contexts can be grouped into different areas of life as, for example, work, public authority, shopping, leisure or health care. Areas of life are sufficiently distinct domains of social interactions that fulfil a particular purpose (for the data subject) or function (for society). Areas of life are thus defined mainly by the relation of an individual to the society.

2.4 Digital Footprint

The term “digital footprint” in this deliverable refers to the definition developed in PrimeLife work package 1. Individuals engage in social and economic life and during their lifetime act in many different areas of interaction, such as worklife, leisure, financial services, healthcare, or governmental services. Every person leaves an enormous amount of digital traces during her lifetime. Each action or transaction that is electronically performed or supported provides an information log. For instance shopping and paying with a bank card or credit card, all Internet actions (browsing, click trail), electronic toll systems, etc. The thousands of data together form a digital footprint of the individual. The data contained in the digital footprint can be created by the concerned individual herself, for instance in the above mentioned transactions or when someone creates a profile page on a social networking service (SNS), or the data can be created by others, such as governmental bodies or businesses.

Furthermore, these data contain partial identities in different areas of life as shown in Figure 1 below [ClKo01]:

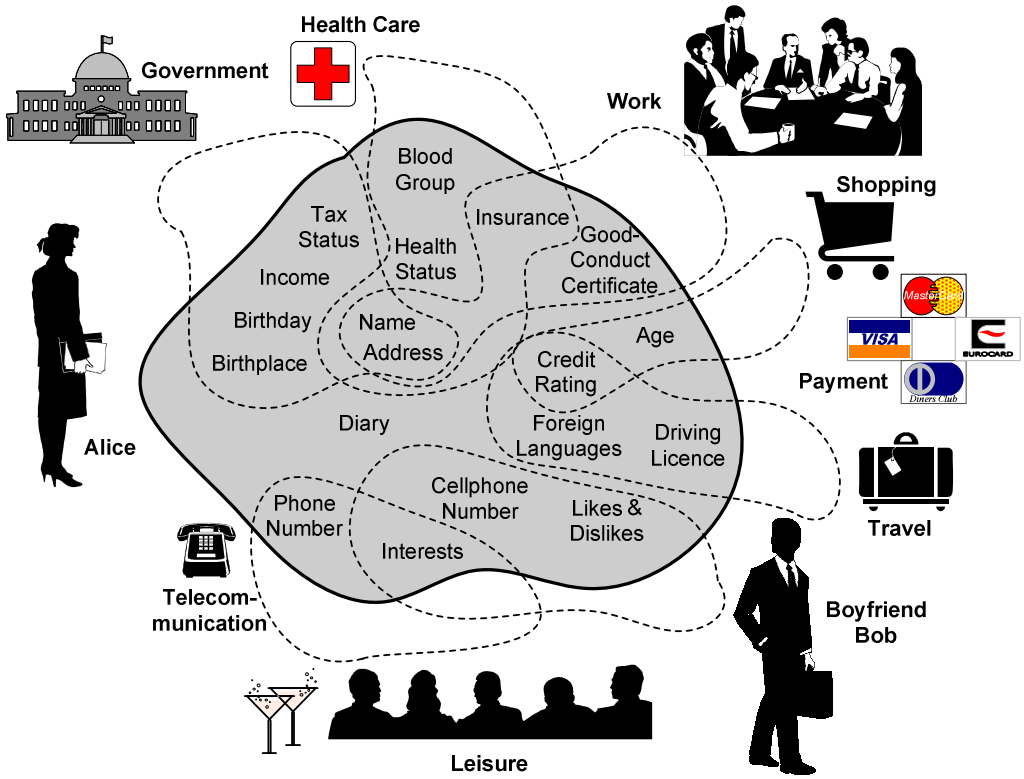

Figure 1: Partial identities of Alice [ClKo01]

Digital footprints are personal data of a person that accumulates in information systems. Most people are unaware of this information and the specific type of information that may be available online. It is also a matter of awareness to get digital footprints visible and inform the user about personal data stored in the web (or in databases). As stated in previous PrimeLife deliverables, ideally only the concerned individual herself should be able to access her digital footprint. The PrimeLife prototype ideas “Show my digital footprint”, “Remove my Digital Footprint” and “Central Data Handling Repository” try to realise a first approximation of such a service.

This chapter shows how digital footprints (personal data of a person that accumulates in information systems or in databases) of persons may appear and develop within someone’s life and relates them to lifelong requirements. It is important that persons get legally and technically the opportunity to control their digital footprints, for example, by deleting parts of them or by encrypting parts of the digital footprint. It should be noted that probably most of the data in one's digital footprint qualify as personal data because of their context or the combination with other data in a data set, which makes it possible for the data to be indirectly linked to an individual.

Chapter 3

High-level requirements for Privacy4Life and lifetime-aspects from the "Seven Laws of Identity"

This chapter recalls the objective of data protection and privacy regulation in terms of high-level requirements for Privacy4Life as well as Kim Cameron's "Seven Laws of Identity" [Came05] under the aspect of an individual's whole life. The chapter refers to legal provisions that regulate these objectives and derives high-level requirements. These requirements focus on general principles which describe what should happen with privacy-relevant data and what should not happen with these data. The following chapters, especially Chapter 4 will seize upon these general principles by adapting them to more specific scenarios or perspectives to derive further requirements. The examination of Kim Cameron's "Seven Laws of Identity" tries to analyse to what extent the "laws" are applicable to the individual's life and relates them to the high-level requirements.

3.1 High-level requirements for Privacy4Life

In this section, high-level requirements regarding transparency, data minimisation, fair use, data subject's identity management as well as change management are analysed. But also the high-level requirements regarding practicability of mechanisms and data handling policies are discussed to help to prevent further risks because of mistakes in data processing and on exercising one's rights.

High-level requirements are derived from changes in society, law and technology. This relates to the implementation of data protection management systems by data controllers to ensure legal compliance and the state of the art in ICT security over time or the reaction to social changes with regard to legal and technical aspects. Societal changes also need to be considered with regard to legal and technical aspects. They have to be recognised and appropriate technologies or legal regulations have to be taken into consideration. Furthermore the assessment of technology and regulations may guarantee a kind of quality assurance.

For the processing and handling of personal data some general characteristics and requirements can be derived from the Directive 95/46/EC as well as the OECD Guidelines on the protection of Privacy and Transborder Flows of Personal data [OECD80].

If privacy has to be considered over a long period of time, some problems will emerge:

- **Technical:** Proclaiming that a certain cryptographic technique will be good enough for 40 years or more, is considered to be ridiculous.
- **Legal/sociological/political:** In a time of 40 years or more, laws, regimes and structure (i.e., common ideas) of society can change drastically (cf. [SeAn08]). What can be regulated by law, politics, and social pressure, might change.
- **Societal:** The concept of privacy, i.e., what is considered to be private or sensitive, might change over time. This implies that revocability of techniques might also be necessary.

In a long-term setting there surely will be some dynamics in policy: both the policy of society at a larger scale and the quite individual policy of a human being in relation with interaction partners [CHP+09]. This poses challenges for technological solutions, in particular:

- Which aspects of technology, which rules implemented in technology need to be addressable by such dynamic changes?
- Which aspects must not be changeable, thus allowing the individual to trust that her expectations will be met, no matter what?
- What are the abusive potentials of new technologies, if not used in a way that one had in mind in the first place?

The starting point of the elaborated high-level requirements is the situation of today: There appears to be at least a common basic understanding of privacy and a consensus that the current baseline will never change, at least in democratic societal models. However, all solutions will have to cope with upcoming changes and cannot – and should not – freeze the status of today.

3.1.1 Openness, transparency, notice, awareness, understanding

Transparency is one of the general principles in our society and also with respect to privacy. It is a necessary principle for estimating privacy risks and decision making concerning privacy-relevant issues, and it is also a prerequisite for further action such as asking all data recipients for access to one's personal data or requesting their erasure. Thus, it is one of the main principles with regard to the data subject's rights, and many requirements within this text will refer to transparency. As it is stated in the Directive [Euro95, Art. 6] that Member States shall provide that personal data must be processed fairly and lawfully, which also means that the data subject must be informed about all data collected and processed about him. Therefore transparency has to be ensured with regard to data processing (data flow, data location, ways of transmission, etc.) in respect of users of the product or service as well as data subjects. An informative, up-to-date and understandable, well-searchable description of the product or service has to be provided to the user (who has to get simple access to those provisions). The data subject has to be informed to whom data are further processed.

Transp-Req: For all parties involved in privacy-relevant data processing, it is necessary that they have clarity on the legal, technical, and organisational conditions setting the scope for this processing (for example, clarity on regulation such as laws, contracts, or privacy policies, on used technologies, on organisational processes and responsibilities, on data flow, data location, ways of transmission, further data recipients, and on potential risks to privacy).

The right to informational self-determination furthermore includes the right to know, who knows what about the data subject (Art. 15 of the Directive [Euro95, Art. 15]). With regard to this, Art. 12 furthermore states, that the data subject has the right to obtain from the controller knowledge of the logic involved in any automatic processing of data concerning him.

3.1.2 Data minimisation

One of the general principles and one of the high-level requirements that aim at ensuring privacy for life is data minimisation. In general, only a minimum of data, strictly necessary for a particular activity and strictly relating to a purpose of processing, should be processed. Because of the general character this principle appears permanently in several stages of life.

Personal data disclosure should be limited to adequate, relevant and non-excessive data as stated in Art. 6 (1)(c) of the Data Protection Directive [Euro95, Art. 6]. It means that data controllers may only store a minimum of data that is enough to run their services. Implied in this requirement is that data needs to be provided on a need-to-know basis and stored in a need-to-retain basis. This requires the requester to specify the purposes of collection, processing and storing of data. Data should be deleted after the requestor's end as soon as the specified purposes of data collection are met. Data minimisation (incl. prevention of undesired linkage and linkability) in general covers the facets minimal quantity, minimal timeframe and minimal correlation possibilities:

Minimal quantity – limiting disclosure: only disclose those data that are strictly necessary for fulfilling the given task. Data not necessary for the given task should not be disclosed or even retrieved. After fulfilling the particular task necessary data should be erased if there is no legal or consented purpose for further processing.

Minimal timeframe – limiting availability: after usage, data should be discarded. To enforce this, legal, organisational and cryptographic tools can be used. Default retention times after which the data are automatically deleted if not specified otherwise have been proposed, for example, for content on the Internet [Maye07].

Minimal correlation possibilities – limiting linkability: advanced data mining technology can allow data controllers to construct links between different partial identities of the same entity. The entity can try to prevent this by running the same data mining technology, upon requests to provide information. This assumes however the same knowledge as the data controllers, which might include invisible links between them (for example, one data controller acting under different pseudonyms). Data controllers might also try to construct links between partial identities of different entities. From a data subject's point of view, this is very hard to protect against.

DatMin-Req: Data minimisation means to minimise risks to the misuse of these data. If possible, data controllers, data processors, and system developers should totally avoid or minimise as far as possible the use of (potentially) personal data, conceivably by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible. Policy makers should implement the data minimisation principle in their work, be it in law making or technological standardisation.

3.1.3 Fair use – Controllable and controlled data processing

The principle of fair use is mentioned in the Directive [Euro95] as well as the OECD Guidelines [OECD80]. There is no clear definition of "fair use", but the core principles of fair information practice are defined as notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress. The OECD Guidelines, for example, point out, that there should be

limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject [OECD80, No7]. Art. 6 of the Directive demands, that Member States shall provide that personal data must be processed fairly and lawfully [Euro95, Art. 6]. In general for all parties involved in privacy-relevant data processing, the processing should be controllable and controlled. The respective responsibilities must be clear, and accountability of the parties involved for their privacy-relevant actions is important. The data processing should be compliant with the relevant legal and social norms.

Control-Req: For all parties involved in privacy-relevant data processing, the processing should be controllable and controlled throughout the full lifecycle. It should be compliant with the relevant legal and social norms.

3.1.3.1 Consent and revocation

Consent and its revocation is one of the main issues that influence the digital footprint of the data subject. The data subject's consent as defined in the Directive [Euro95, Art. 7a] is one of the most common legal bases for processing of personal data. The Article 29 Working Party elaborated on the preconditions of a valid consent in its working paper and identified four preconditions: consent must be a clear and unambiguous indication of wishes, consent must be given freely, consent must be specific, and consent must be informed [Arti05].

In general, users' data should only be accessible to authorised third parties. These include parties that are legally allowed to access the information (secret service, descendants, doctors), or that have been given consent by the data subject. Given the large time-frame, data subject's consent should be limited in time by default (for example, the consent given by parents for their children is limited until children reach legal age and become autonomous to decide about the consent). In addition it should be made clear what will happen if the person who has consented dies – in some cases this will be equivalent to the withdrawal of the consent, in others the person who died may explicitly want his consent to survive for an additional time-frame (for example, as part of the specific legacy). Moreover, it remains to be defined to which of their data minors are allowed to give consent to others (some of these "rights" might also be attributed to their care-takers[10]). Consent should not only be limited in time, but it should be made clear which parts of the planned (and to be consented) data processing is not revocable and what will happen (how quickly) when the consent is withdrawn. Finally there are also situations that do not allow giving individual consent, for example, if the data subject has no possibility for an autonomous statement (e.g. conscious consent) [Simi06, §4a].

In principle data subjects have the right to withdraw their consent at any time. However, revoking one's consent does not imply that the consequences of data processing can also be revoked: The past cannot be altered; data disclosures cannot be "undone". The revocation comes only into effect for the future and only regarding the data controller the withdrawal of consent is communicated to. In practice, the data controller may already have transferred the data to other parties (this may or may not be legally compliant), or because of a data breach the data may have become known by others. The revocation of consent regarding the primary data controller does not affect these further data disclosures. Also, consequences based on the disclosed and now withdrawn data don't become automatically invalid. This shows that revocation of consent is often a merely theoretic concept. Therefore consent should not only be limited in time, but it should be made clear which parts of the planned (and to be consented) data processing is not revocable and what will happen (how quickly) when the consent is withdrawn.

[10] See below, Section 4.4.1.2.

3.1.3.2 Purpose binding

Part of the fair use high-level requirement is also the principle of **purpose binding**, stipulated in Art. 6 (b) of the Data Protection Directive [Euro95, Art. 6b]. Personal data should be relevant to the purposes for which they are to be used and to extend necessary for those purposes, should be accurate, complete and kept up-to-date [OECD80, Part 2, 8]. Binding to context might be done in two ways: limiting/prohibiting the use outside the given context, or making the context stick to the data (sticky context could be seen as the meta-data of a sticky policy). Well-documented sticky policies might capture both (context) concepts. Purposes for which personal data are collected should be specified no later than the time of data collection and the subsequent use limitation (called downstream usage in D5.1.1) to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose [OECD80, Part 2, 8]. The purpose limitation has central importance for business, since it attempts to set the boundaries within which personal data may be processed, and those within which data collected for one purpose may be used for other purposes [Kune07, 2.89, p. 99]. The purposes for the collecting and processing of personal data have to be stated clearly within the privacy policy. Furthermore, data must not be used for further purposes incompatible with the original purposes once they have been properly collected. The data subject has to give his consent for every change of purpose.

3.1.3.3 Sensitive data

Within one's whole life many **sensitive data** are collected and further processed and therefore subject of the fair use high-level requirement. The more personal and especially sensitive data are included within the digital footprint, the more complete is the picture of a person within the web. Sensitive personal data are specially protected within the Directive [Euro95, Art. 8] and the processing of sensitive data is prohibited, except under certain clearly-defined circumstances such as when the data subject has given his explicit consent. Over the lifetime of the data subject, the digital footprint may rise and may be accumulated with sensitive data. This should not happen especially without the data subject's explicit consent or on a legal basis, because it raises the possibility of linkage.

3.1.3.4 Dealing with conflicts

With regard to the fair use high-level requirement, there may occur situations with **conflicts** between different rights of data subjects. For instance, the fundamental right of freedom of speech can prevail the right to privacy as a legitimate interest, also for opinions voiced on the Internet. In German constitutional law a differentiation is made between opinions and facts. Voicing true facts is usually lawful. Voicing opinions is usually lawful, as long as these opinions are not offensive or abusive. A balancing exercise is necessary between the conflicting principles of Art. 8 ECHR (right to privacy) and Art. 10 ECHR (right to freedom of expression) to be performed by courts on a case-to-case basis [ECHR50]. Publishing opinions and facts with mostly personal data has fundamental effects to the digital footprint of a data subject. As voicing opinions is usually lawful, the effect to the digital footprint is also lawful and therefore the data subject can not claim any infringement. But if a balancing of interest is necessary, the data subject may claim against the publishing of data and therefore control his or her digital footprint.

Conflicts of interest furthermore appear when data subjects or controllers are protecting private data while others want to access it. A first remark that can be made here is that this is not necessarily a conflict in which the data subject is involved. Parties that do have legitimate access to the information (for example, hospitals) could refuse access to these data to other parties (national health department trying to control a new pandemic). Even if they would be willing to

provide the data because it would serve a good purpose, they might be prohibited by law (or even by their own privacy-preserving technology). In case of emergencies, specific "breaking the glass" policies [Pove99] should be available. In some cases, government/legal actors can intermediate in conflicting interests, using regulations. Automated resolution of conflicts seems to be undesirable [Euro95, Art. 15], but an automated way of notifying users and data controllers that a conflict exists, and technological tools to facilitate negotiation to receive consent seems useful.

Conflicts may also derive from handling "shared data". Some personal data may affect not only one data subject, but several (cf. [Phil04], [LaRo08]). Therefore it has to be clarified how the processing of shared data can be treated by the data subjects concerned. This can be done by technical mechanisms as well as legal solutions, such as clear regulations regarding consent in the processing of shared data.

3.1.3.5 Lifecycle of data and processes

For all data and processes, controllability of full lifecycle is needed: When creating data items or accounts and starting up processes, the deletion of the data items should be anticipated and planned. This is important for data controllers with their professional data processing as well as for individuals who disclose data in a social network or setting up an account somewhere. Not only the existence of data has to be considered, but also its linkability to other data items (cf. Section 3.1.2). This is especially relevant when introducing unique identifiers. Planning the lifecycle also encompasses the definition of procedures for answering user requests (for example making use of right of information) or emergency settings in case of data breaches [Mein09].

3.1.3.6 Data subject rights

The fact that data subjects do leave digital footprints in the web, also means, that the data subject has certain rights on the data she left within the digital footprint, such as the general rights stipulated in the Data Protection Directive [Euro95, Art. 12ff].

Apart from the data subjects rights the discussion point here is to what extent the disclosure of data by the data subject implies consent for processing of personal data and whether these public data are available for all purposes as fruits of the public domain. This question can be answered with the provisions of the Data Protection Directive where Art. 6 states, that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes [Euro95, Art. 6]. The data subject's consent can be implied for the purposes that are visible for the data subject when giving the consent. If personal data is further processed, even as fruits of the domain, there may be a change of purpose that requires a new consent of the data subject or any other legal basis. Even publicly available personal information has to be used carefully. If one wants to further process these data he needs to assure that this processing is legally allowed (legal basis needed), otherwise the protection of personal data may be undermined.

Most of the data subject's rights are stipulated under the provision of the Data Protection Directive [Euro95], but also the provisions of the ePrivacy Directive [Euro02] may be applicable in cases where electronic communications services are provided. If the ePrivacy Directive is applicable, further rights of the user may be taken into account, for example, Art. 6 (4) whereas the service provider must inform the user of the types of traffic data which are processed and of the duration of such processing for the purposes determined. Furthermore it has to be kept in mind that the definition "user" in the ePrivacy Directive means any natural person using a publicly available electronic communications service, without necessarily having subscribed to this service [Euro02, Art. 2a]. In most of the cases the data subject and the user coincide and both provisions are applicable.

3.1.4 User-controlled identity management

In general, the data subject shall have full controllability for all data and purposes within the full lifecycle. A subject's data should be protected for life. This means that each data item should be traced during its life-cycle. When creating data items or accounts and starting up processes, the potential impact on other partial identities should be measured and presented to the data subject for evaluation (evaluation can be partially automated or automatically documented). Moreover, controllability assumes that the information, presented to the data subject is understandable. Finally, deletion should be anticipated, and the desired degree of deletion determined: complete deletion assumes that copies held by data controllers are also deleted, and that secondary usage might not be allowed for such data.

The essence of PrimeLife's approach to identity management builds around the postulation of data subject centricity. The aim is to put the data subject of (new) information technologies (in an online world), egovernment services, and offline services facilitating processing of personal data in control of the data processing occurring. The approach of user-controlled identity management as well as of exercising informational self-determination presupposes that the acting data subject fully comprehends the effect of the data processing in question. As described above, transparency is an essential prerequisite for exercising the right of informational self-determination. In order to understand the information given, make a decision as to allow or prohibit the intended data processing and act accordingly and voice this decision, a certain degree of sanity as well as mental maturity is required. With regards to fundamental rights it is possible to distinguish between a "legal capacity to bear a fundamental right" (Grundrechtsfähigkeit) and "the ability to exercise a fundamental right on one's own" (Grundrechtsmündigkeit).

Every natural person bears the fundamental right of informational self-determination. However, every natural person during his or her lifetime passes through (a) stage(s) during which s/he does not have the ability to understand the consequences of data processing conducted by data controllers, or s/he is not capable to exercise self-determination via the provided means, for example, due to usability problems. In general, one's life can be classified in three large stages of childhood, adulthood and old age, as shown in Figure 2 [CHP+09].

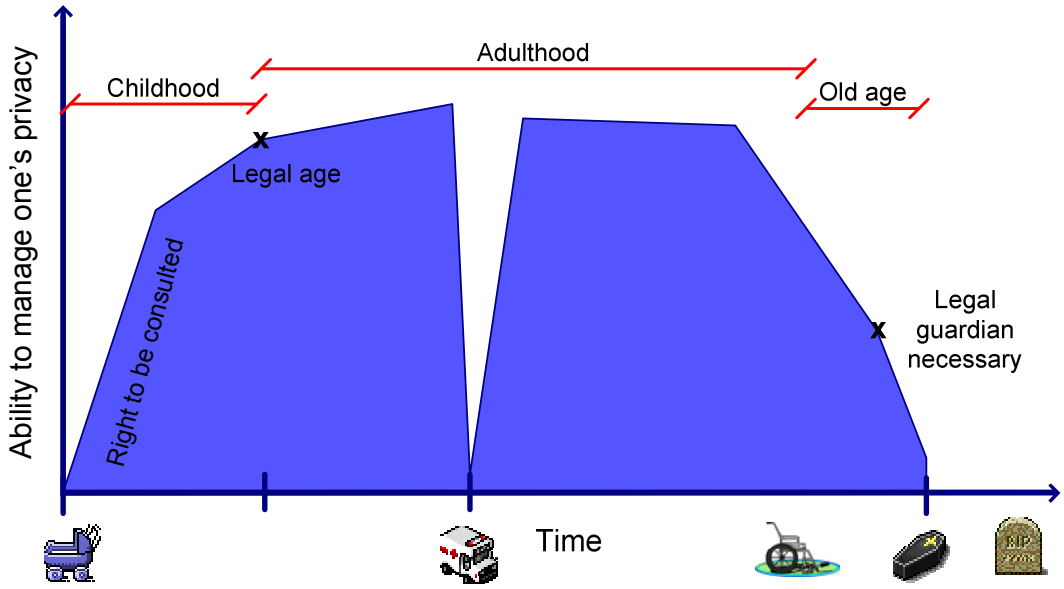

Figure 2: Exemplary stages of life [CHP+09]

3.1.5 Practicability of mechanisms

Usability can also be defined as one of the general principles. Interfaces have to be well comprehensible for data subjects. If personal data are stored in many different contexts, provided they are all well protected in functional differentiation, how is control and oversight maintained? Provided having an identity management system of full support of partial identities, it still seems very hard to differentiate the different partial identities and to avoid linking. A challenge will be to simplify the view for the data subject on her partial identities, the performed transactions and (potential) linkage of disclosed data without oversimplifying which may mean to hazard the consequences of wrong privacy-relevant assumptions the data subject derives.

In general, there might be certain conditions for mechanisms. Mechanisms need to be practical, viable, functional, helpful and useful for individuals to prevent further risks because of mistakes in the data processing and for the exercising of one's rights.

3.1.6 Dealing with changes – change management

When enabling identity management throughout life, one has to take into account how to deal with changes in society, law and technologies. This not only relates to the data subject, but also affects data controllers and processors. Data controllers, for example, have to ensure legal compliance over time as well as the state of the art in ICT security by implementing data protection management systems. The question here is how appropriate reaction to social changes may be enabled with regard to technical and legal aspects. Changes have to be recognised and collected before new technologies may be developed or new regulations may be stipulated to ensure quality assurance.

ChangeMng-Req: Data controllers, data processors, and system developers should monitor changes in society, law and technologies and react appropriately (for example, by evaluating chances and risks, adapting current processes, regulation or standards to the changed conditions etc.).

The Directive lists six potential legal bases for data processing [Euro95, Art. 7]. Mostly the processing of data bases on a contract of user and controller or the consent of the user. This raises the question what happens if the legal basis changes. As the data controller is liable for the legal compliance of the processing of personal data, he has to install data protection management processes (in addition to security management processes) to monitor and react to possible changes [Mein09]. Among others, the controller may have to inform the data subject about the change of contract and has to ask for a new consent to the changed contract.

3.2 The "Seven Laws of Identity" in the spirit of Privacy4Life

This section examines Kim Cameron's "Seven Laws of Identity" [Came05] under the aspect of an individual's whole life. Life situation and age have an implication on Identity Management [HaPS08]:

- Babies are represented by their parents,
- Kids start to have their own identity,
- Teenagers act in most things on their own behalf, they usually even have multiple digital identities [Boyd08],

- Adults fully act on their own behalf,
- Elderly start depending on other persons,
- To some extent the heirs even deal with somebody's identity even if that person already died.

The goal of this section is to contribute to the broad discussion of the "Laws of Identity" which intents to "harden and deepen the laws". This section takes up the "Laws of Identity" to see to what extent they are applicable on the individual's life. It is neither planned by this text to extend the "Law of Identity" with extra "laws", nor is it expected that the "laws" need to be redefined. But, we expect that this discussion broadens the general understanding of the "laws".

Privacy-enhancing identity management has been researched for almost three decades, refer for instance to [Chau81], [Chau85], [Chau92] and references in [PfHa08]. One prominent result of research in identity management is the formulation of the "Laws of Identity" by Kim Cameron [Came05], which underwent open and broad discussions by the research community. The paper "define[s] a unifying identity meta-system that can offer the Internet the identity layer it so obviously requires." [Came05, p. 1]. This identity metasystem offers in a generic yet applicable approach how an identity system should be built to be secure, user-centric, and manageable. The general idea is to create "a unifying identity metasystem that can protect applications from the internal complexities of specific implementations and allow digital identity to become loosely coupled. This metasystem is in effect a system of systems that exposes a unified interface much like a device driver or network socket does" [Came05, p. 3].

In contrast, [HaPfS08] points out that "current concepts for identity management systems implicitly focus on the present (including the near future and recent past) only. The sensitivity of many identity attributes and the resulting need to protect them to enable privacy-aware identity management throughout the whole life is currently not dealt with" [HaPfS08, p. 3]. This is also true for the "Laws of Identity". They implicitly assume a well-educated user, healthy and being able to take care for her own privacy. [HaPfS08] show that people`s current living conditions, age, and health condition have deep implications on the ability to deal with their digital identity. They look at three aspects that should be covered by privacy-enhancing identity mechanisms: all areas of life, all stages of life, and the full lifespan (cf. Chapter 2).

"Areas of life" refers to a way an individual handles her various partial identities [PfHa08]. People act in different roles and in various contexts, for example, patient in a health care system, student in an education system, or member of a sports club. *"Stages of life"* refers to the individual's personal development from birth over early childhood, youth, adulthood to late years and death. Each of these stages has different requirements on identity management, primarily with respect to delegation of identity-related decisions. For instance, infants are represented by their parents, while teenagers act in many things on their own behalf, they usually even have multiple digital identities [CLG+08]. The aspect of *"full lifespan"* emphasises that identity systems have to serve a user over a very long period time, i.e., typically a lifespan over several decades. The use of an identity does not stop with the death of the data subject, because to some extent the heirs and officials even deal with somebody's identity even if that person has already died. The metasystem may even evolve during that time, but it needs to be able to cope with user's partial identities from all stages in life. That means it has to be backward compatible to some extent to deal with identity tokens the data subject created or collected decades ago. Today, there is very little experience with long-living software systems in general [Parna94], with cross-areas of life spending software in particular, let alone with long-living identity systems.

We review the "Laws of Identity" to see how they have to be applied to lifelong identity management. The authors think that the research community needs a discussion which broadens the general understanding of the "Laws of Identity" taking into account that selected partial identities may last decades and will be in use even beyond the lifetime of the data subject. In order

to start this discussion we will discuss the seven "Laws" one by one under the introduced concepts of Areas of Life[11], Stages of Life and Full Lifespan. From this contemplation we will draw conclusions on how an *identity metasystem for the full lifespan* could look like.

3.2.1 Law 1: User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent. [Came06, Law 1][12].

The first (and from our perspective most fundamental) "Law" defines that the data subject is ultimately the controlling instance of her own identity information. Identity systems have to get data subject's consent before they disclose any personal information on her behalf.

This certainly implies that the individual is actually in the position to consent. Looking at the various aspect of privacy throughout lifetime this is not always the case. The data subject may be in a stage of life where she cannot consent, for instance as a small child or as a very old person. The data subject's consent may also be requested in an area of life which prevents her from doing so, for example, acting as a patient in the health care system while she is unconscious or otherwise unable to consent.

We can distinguish the reasons for not being able to consent in two groups: it might be a temporary reason or a permanent reason. A temporary reason vanishes after a reasonable amount of time and the user gets back in control of her own identity metasystem. The amount of time being reasonable may depend on from the context of the identity-related operation. In case of permanent reasons the data subject needs a proxy that acts on her behalf. Certainly, it is fair to ask why a data subject being permanently disabled to consent does use an identity metasystem in the first place. But the data subject could have collected partial identities before she got permanently disabled to consent, or there are areas of life which impose a partial identity onto the data subject, for example, electronic tax record systems. Moreover a permanent reason could become a temporary reason, for example, after a data subject recovers from a serious illness or a child grows up and takes control over her own identity metasystem.

We propose, that "Law" 1 should be interpreted in a way that the condition "with the user's consent" includes the consent given by a proxy on behalf of and in the best interest of the data subject. Appointing a proxy might in a lot of cases imply legal considerations. Ultimately, the proxy needs at least partial access to the data subject's identity metasystem. The proxy must be able to review identity transactions, consent for submitting personal information, or even being able to create new partial identities for the data subject. As in real life, different types of proxies might be necessary ranging from fully trusted proxies to proxies being empowered for specific partial identities and specific transactions only. Moreover, the data subject may want to appoint different proxies for different partial identities.

"Law" 1 demands "translucent" [Came05, p. 7]; the identity of the receiving party needs to be verifiably correct and the system has to "make the user aware of the purposes for which any information is being collected" [Came05, p. 6]. Both principles should be true for the data subject's proxy as well. In the explanation of "Law" 2 Cameron demands that "every party to disclosure must provide the disclosing party with a policy statement about information use. This policy should govern what happens to disclosed information" [Came05, p. 8]. This supports our

---

[11] See below Chapter 5.

[12] We quote the Laws in the section headings from Cameron's website [Came06] since the phrasing underwent a throughout discussion in the "Blogosphere" and is therefore more mature than in the initial publication Cameron (2005).

statement that transactions (made on behalf of the user) need to be traceable for the data subject. The user should be able to verify at later points in time which information the proxy disclosed, to whom and for which purposes.

This has a strong impact on the architecture of the identity metasystem. At a first glance this looks like a role-based access control policy would do the job. The proxy's identity gets associated with a role being associated with permissible actions on the identity data. But if the data subject is not able to consent to a simple transaction, she is even less in the position to change this policy to give the proxy access. We have to understand that a proxy model does not solve all problems, but could even introduce new problems. For instance, the proxy is associated to the data subject which could induce linkability [PfHa08] and enable discrimination.

Having said all that, there is even more that needs to be considered, which is maybe not solvable by a proxy approach at all [CHP+09]. An important point is that the user needs to understand the long-term consequences and must be able to revoke consent later on – be it given by a proxy or in person. Revocation of course may or may not change the consequences of the earlier decision (cf. Section 3.1.3.1). There may even be situations where the data subject consented, but the given consent must not count since this would be "contra bonos mores" (against public policy). Finally, there are situations where consent is not needed at all, namely if this is regulated accordingly in the law or in a contract, for example, in severe cases of misuse.

It seems that this interpretation of the first "Law" needs to be addressed not only by technology, but also by social, organisational and legal considerations.

3.2.2 Law 2: Limited Disclosure for Limited Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable, long-term solution. [Came06, Law 2]

The main idea of the second "Law" is to disclose as little personal information of the data subject as possible. Cameron argues that "aggregation of identifying information also aggregates risk. To minimize risk, minimize aggregation" [Came05, p. 6]. This means that the user should disclose at any given interaction with a service the "least identifying information".

However, not all information has the same potential of identification. On one hand some small portion of information could be sufficient for lifelong tracking a person, whereas on the other hand some attributes may change during life-time, for example, hair colour. So an identity metasystem adhering to the second "Law" should help the data subject to distinguish between information with high and low long-term potential for identification.

If an identity relationship exists over a longer period of time, there is the risk that the user leaks linkable information bit by bit. One approach to avoid that is that the user should provide always the same token as in previous interactions. This in fact means that the data subject would need to track which claims she presented to a third party when and why. This fits to the notion of privacy throughout all areas of life. The data subject would need an activity record for all her partial identities. Another approach would be utilising unlinkable tokens. In this case the identity metasystem should make sure that it generates a fresh token for each interaction with the third party.

Despite the limited disclosure, the second "Law" already highlights that the identity metasystem needs to be a "long-term solution". With regard to the aspect of full lifespan in [HaPS08] this means at least 80 years. So far, there is no experience with such long-living IT technology [Parna94]. Certainly, we cannot be sure that the Internet as we know it today will stay over this long period of time; maybe it will be replaced by a network offering a proper unified identity layer. But since it is very expensive to exchange a global-scale infrastructure, we assume that the Internet will survive and at least part of its services the user utilises today, too.

Collecting claims over this period of time means that the data subject is accumulating identity tokens in many different data formats. The identity metasystem is described as "system of systems […] that exposes a unified interface much like a device driver or network socket does" [Came05, p. 3]. This means that the data subject is not only collecting the identity data but also identity subsystems (for example, drivers, plugins, and executables) that are able to decode specific identity tokens. This leads us to an extended backup problem – not only the claims but also the identity drivers need probably to be accumulated and backed up for a long period of time.

In the course of several decades, technology changes drastically. Cryptographic tokens get less secure due to the availability of extensive computing power and new cryptanalysis results. To tackle this problem the identity providers should reissue claims with stronger keys or based on different cryptographic principles from time to time. The identity metasystem would be an ideal place to trigger reissuing of claims periodically. The user should be warned if claims have not been changed or reissued for a given period of time.

3.2.3 Law 3: Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. [Came06, Law 3]

This third "Law" essentially demands that an identity relationship should have a minimal number of involved parties. Each participation shall be justifiable. This applies also to the proxy acting on data subject's behalf. They also need to be justifiable, which means they should not be able to interfere if the data subject does not need them.

One way to limit malicious interactions by proxies is to apply the principle of mutual control. The data subject defines that specific interactions are only possible when *n* out of *m* proxies consent [Pove99, p. 41]. The underlying assumption is that less than *n* proxies collude in a malicious interaction. The most common setting would be a four-eye principle where two proxies unanimously consent. We have similar settings in real life, for example, when official forms need to be signed by both parents.

Another interesting aspect is applying *breaking the glass policies* [Pove99, p. 41] in an identity metasystem. This technology is often discussed in health care scenarios [FCA+06]. While the user wants to keep his medical health record private, he gladly allows a stranger to access it in case of a medical emergency. A simple example for a breaking the glass policy would be: *"proxy pays the user €100,000 for disclosure of user's private information; the user pays the proxy €100,000 when disclosure of private information was necessary and justifiable"*. In case the proxy discloses information right-fully both money transactions equal out, nobody has to pay anything. In case of malicious disclosure of private information the proxy has to pay.

3.2.4 Law 4: Directed Identity

A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for private entities, thus facilitating discovery while preventing unnecessary release of correlation handles. [Cameron, 2006, Law 4]

The fourth "Law" advocates that it must be the data subject's choice if an identity is widely known within a set of identities, for example, "the examples in an enterprise, some arbitrary domain, or a peer group" [Came05, p. 8]. It must be up to the individual to decide whether she wants to establish an "identity relation" with another identity or not. This touches again our point that proxies have to decide this for the user not being able to take this decision. Proxies acting on behalf of the data subject shall not be able to switch a partial identity from unidirectional mode to omnidirectional. Limiting a proxy's permission with respect to the fact how visible data subject's

identity is after a transaction seems very challenging. It anticipates that the proxy knows in advance what the communication partner is going to do with data subject's disclosed personal information, i.e., publish it vs. keep it confidential. Automatic evaluation of the peer's privacy policy could help the identity metasystem to take a permissive decision whether the proxy may decide about this or not.

3.2.5 Law 5: Pluralism of Operators and Technologies

A universal identity metasystem must channel and enable the interworking of multiple identity technologies run by multiple identity providers. [Came06, Law 5]

The fifth "Law" states that a universal identity metasystem must embrace different technologies. Under the aspect of full lifespan this means that the technologies are not only "multiple", but really technologically diverse.

Assuming that the market would offer different identity metasystem technologies that are all interworking, it is an interesting question if users actually understand that all these diverse experiences are technically equivalent. Another interesting aspect is to use the paradigm of "Law" 5 for technological evolution. Since the underlying protocols stay the same, the market could offer ever enhanced versions of identity metasystems. That could realise a smooth transition between technology generations. However, from the experience with today's systems we know that a standard never stays untouched for a long period of time. Either it is used and adapted or it is abandoned. Since identity is something with a long-term aspect, we would need to find a way to make "Law" 5 stable and applicable for at least several decades.

Considering multiple technologies for the stages of life, this would allow offering access to identity information in the most user-friendly way, i.e., a child would get a different user experience than a grown-up or elderly person. The interworking protocols make sure that all identity metasystem clients can exchange information among each other. A proxy could get a user experience that is specialised in the area of life, she is representing the user in. For instance, a proxy for legal affairs may have a different user experience than a proxy in a private area of life, such as a sports club.

3.2.6 Law 6: Human Integration

The unifying identity metasystem must define the human user as a component of the distributed system integrated through unambiguous human-machine communications offering protection against identity attacks. [Came06, Law 6]

The human user is recognised as the central point in an identity metasystem and even "must define the human user to be a component of the distributed system" [Came05, p.10]. The sixth "Law" stresses that user's experience has to become "predictable and unambiguous enough to allow informed decisions".

Applying this principle to the lifetime aspect reveals two aspects. First the data subject needs to understand what was happening when he was not able to make a conscious decision. The data subject may appoint many proxies for each of her partial identities to ensure an *n* out of *m* voting schema as discussed above. Thus the "user" in Cameron's case would become a plurality of users being involved in decision making. It would be very interesting to see how a user experience looks like that involves multiple stakeholders. Does each proxy, for instance, see how the other proxies voted? Do the proxies have a communication channel that allows discussing the data subject's will and the implications of a decision?

Another aspect is the evolution of a user experience over the full lifespan of the data subject. "Unambiguous human-machine communication" is crucial to keep the elderly and people with

low education as long as possible able to act on their own behalf. It is a key differentiator to keep the group of self-acting people as large as possible. This is not just a matter of user interfaces, but also of properly selecting and communicating the general concepts and mental model. In principle the identity metasystem needs a way to adapt to advancing state of the art, i.e., updating the user experience from time to time. However, a regular update of the user experience could be counterproductive looking at the age and mental flexibility of the data subject. An elderly person might be very confused when the user experience she knows suddenly changes, even if it is for best reasons, and in effect stops using the identity metasystem completely. Updating the metasystem's user experience leads to a variety of user interfaces that co-exists in parallel and they might differ not only in visual appearance, but more fundamentally in the utilised mental model. This is very much comparable with ever new versions of operating systems; they co-exist for a while and one can observe that users are hindered to help each other since they might use different versions of the operating system. Certainly, the same applies not only for the user but also for each proxy.

3.2.7 Law 7: Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its user a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. [Came06, Law 7]

Proxies should have a way to separate their personal contexts from contexts of people they are acting for. Please notice the plural of the word contexts. A person may have to act in various personal contexts and in various contexts in the role of a proxy. Hence the identity metasystem should provide a user experience that clearly visualises in which context and on whom's behalf somebody is acting. This even extends the interpretation of "Law" 7, since it does not only need to "provide a simple, consistent experience while enabling separation of contexts" but also for responsibilities. Moreover, whenever delegation of responsibilities is involved, the delegating data subject needs to be able to grant delegation, to see ongoing delegations, and revoke previously granted delegations. This refers back to related statements we made for the first "Law". If the data subject can revoke a delegation, this may have legal implications. Moreover, situations could occur where proxies are not able to make conscious decisions either. Hence, the data subject's proxies suddenly need a proxy. What does that mean for the original user? Is the delegation to the first proxy automatically revoked and how does the data subject learn about this new circumstance? Extending the concept of contexts to other people's contexts is the main demand to this "Law" under the light of lifelong privacy. But this is not an easy task and requires deep discussion.

3.2.8 Lessons learned from applying Privacy4Life to the "Seven Laws of Identity"

We confronted the "Laws of Identity" with lifelong aspects of digital identities, areas of life and stages of life as defined by [HaPS08]. Our main conclusion is that the "Laws" as such seem to hold even if they are applied in this broad context. However, some aspects in the "Laws" have to be interpreted in a slightly different way to make a lifelong identity metasystem happen. Concrete items we mentioned in the discussion of the individual "Laws" are:

- Allow proxies for each partial identity
- Allow multiple proxies with mutual control
- Trigger reissuing of claims to prevent degeneration of cryptographic material
- Backup problem for identity data and associated mechanisms

- Transparency of actions
- Underlying interworking protocols need to be stable for decades
- User experience should be adopted to a person's stage of life
- User experiences have to cover multiple contexts in multiple responsibilities

These requirements map to the high-level requirements we discuss in Section 3.1. The purpose of Chapter 4 is to break those high-level requirements down to more detailed requirement descriptions. Hence, it contains useful thoughts on how a lifelong identity metasystem could actually be implemented.

The most prominent aspect in this review of the "Laws of Identity" is the user-controlled identity management, which is addressed in Section 5.2. This covers the demands that the data subject can make a conscious decision or could delegate such decisions to one or more proxies of her choice (cf. Section 4.4). Data minimisation is mainly the concern of "Law" 2 and it leads to the conclusion that the identity metasystem needs to help the data subject to achieve this minimisation. Sections 3.1.2 and 4.2 take a deeper look in this aspect from a legal point of view. Openness, transparency, notice, awareness and understanding is discussed in Sections 3.1.1 and 4.1 and play an important role for the traceability of user action and the traceability of proxy's action on behalf of the data subject.

Moreover we touched upon certain technological aspects that are of interest, such as pseudonymous convertible credentials (cf. Section 5.3.7) or secure logging of proxy's actions (cf. Section 5.3.10). The referenced chapters give more details about those technologies.

3.3 Conclusion

This chapter shows that there are various high-level requiremens on what should happen with personal data and what should not happen with personal data. It has to be pointed out, that these selected scenarios are not exclusive and represent only some possible aspects where further improvement is necessary within identity management throughout life. With regard to the "Seven Laws of Identity", some "Laws" have to be interpreted in a slightly different way to make a life long identity metasystem possible and they still work even if they are applied in this broad context.

Furthermore the "Laws" impose implementation of responsibilities in the hands of the data subject which is not the aim of PrimeLife. The project however intends to relieve the data subject which leads to the question to what extent responsibilities of privacy and identity management can be left to the individual in general.

Chapter 4

Requirements concerning different actors

This chapter elaborates on who should be responsible for meeting the principle and objectives stipulated in Chapter 3 in concrete situations. Therefore concrete requirements are determined to define what to do and how to react in certain situations. This chapter apprehends to the general requirements and remarks of the previous chapters and furthermore gives concrete guidelines in which situations throughout one's life further improvements may be necessary. Basic requirements of Chapter 3 are to be further continued with regard to requirements that may be necessary. These requirements refer to the responsible persons or institutions, such as the data subject, user, data controller and processor, developer of ICT systems, supervisory authorities, privacy organisations or standardisation bodies.

4.1 Openness, transparency, notice, awareness and understanding

To enhance transparency for the data subject, the service provider can inform the user by providing relevant documentation on a product or service, for example, user manual, security policy or other legal documents. Furthermore the buyer of a product who acts as controller must be informed about all relevant privacy issues. The same holds true for the provider of an IT-based service if users of the service are (co-)controllers of the processing.

4.1.1 Awareness

The requirement transparency is very much related to awareness. First of all data subjects have to be aware of the identities that are created by them in daily life or in the web. The requirement awareness is of special interest, when identities of individuals/users are created about them by others. In these cases individuals are not aware about the existence of formal identities and they do not have any control. Therefore all parties involved in privacy-relevant data processing, in particular data subjects, should be made aware of potential risks to privacy and ways to deal with

these risks, for example, in privacy policies. But it has to be taken into account that too much information may overwhelm the data subject and in this case awareness is also not given any more because the data subject can not use the information properly. Creating awareness also means to find a balance of appropriate information of the data subject. Furthermore, the expectations on awareness may vary in different societies. As society is changing, also the responsibilities may change. But in conclusion the focus should always lie on the data subject. The question on when or who will be informed by whom and how has to be clarified.

Furthermore, the expectations on awareness may be various with regard to different societies. As society is changing, also the responsibilities may change. But in conclusion the focus should always lie on the individual user. The question on when or who will be informed by whom and how has to be clarified.

Transp-Req: Schools or education centres should make individuals aware of potential risks to privacy and ways to deal with these risks.

Transp-Req: Data controllers and data processors should make their employees aware of potential risks to privacy concerning data processing and ways to deal with these risks.

Transp-Req: Parents should make their children aware of potential risks to privacy and ways to deal with these risks.

4.1.2 Transparency of what is irrevocable and what is revocable

In a lifelong context certain information on data subjects needs to be revocable, whereas other information might not be. Legal provisions acknowledge such revocability for personal data, by the right to have data deleted, and also in copyright law, when the author decides so. Therefore the Directive states, that every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified [Euro95, Art. 6 and 12]. The data controller needs to erase or block data that do not comply with the provisions of the Data Protection Directive, in particular because of the incomplete or inaccurate nature of the data.

However, in the case of copyright law, already published material cannot be recalled. The right of the author merely allows stopping further publishing. The material also will be available in archives that already acquired it. In an information society, this might mean that the information is still going to be widely accessible. Clear rules need to be defined that make transparent if and under what circumstances information will be available forever.

Transp-Req: For all parties involved in privacy-relevant data processing, it should be clear under which circumstances decisions are revocable/irrevocable and what the potential impact can be. In particular, data controllers should inform data subjects on to which degree their decisions (such as consent to processing of personal data or distribution of these data) are revocable or not.

4.1.3 Transparency and accountability

The law in some cases already provides provisions, which oblige data controllers and processors to log their processing of data. These logs need only to be kept for a certain period of time, and then need to be deleted.

As log files may contain personal data about the data subject and those who are processing the data, it has to be considered under the lifelong perspective a historical dimension, to allow later access for research purposes and thus data may need to be stored in archives. Sufficient logging mechanisms need to be implemented. There also has to be sufficient information of the data subject what kind of data are stored within a log and for how long the log is accessible under which conditions (for example, within the privacy policy).

Transp-Req: Data controllers and data processors should keep audit trails on the privacy-relevant data processing.

Transp-Req: For audit trails, data controllers and data processors have to define and make transparent (at least within the organisation and for supervisory authorities) which information is logged for how long.

Transp-Req: For audit trails, data controllers and data processors have to define and make transparent (at least within the organisation and for supervisory authorities) who can get access to the log data under which conditions.

Note that there may be the need of a secondary audit trail to log all accesses to the primary audit trail if it contains privacy-relevant data. Of course this cannot be infinitely repeated in a recursive process by introducing a third, forth etc. audit trail, but instead controlling the access of an audit trail may be realised by applying the four (or more)-eye-principle without the possibility of one party to access the data on its own. Also, audit trails should be designed in a data minimising way, e.g., by using pseudonyms so that the log file can be analysed in a first step without directly identifying persons, but offering a second step, e.g., in the suspected case of misuse, where more personal information is provided.

4.1.4 Transparency of the logic behind privacy-relevant data processing

The data subject has a right to know who knows what about him or her. Therefore, the logic behind the processing, especially the processing of personal data with regard to profiling has to be described in detail to guarantee transparency for the data subject. The right of information therefore comprises not everything that is technically possible, but the processing of personal data, which is actually foreseen and controlled by the processor. If personal data are analysed in a statistic-mathematical way, to classify the user by interests or purchasing power, within the constituency, these mechanisms have to be revealed by the processor. Important is the principle of function of the application programme, so the user may understand how the assessment and the classification is derived from his personal data and which relevance the personal information have within the processing system of the processor.

Transp-Req: Data controllers and data processors should inform data subjects about the logic behind data processing (for example, in profiling systems) in a comprehensible way.

Transp-Req: In case other regulation inhibits detailed information for data subjects, data controllers and data processors should make the logic behind data processing transparent for supervisory authorities.

4.1.5 Transparency on linkage and linkability

During an individual's lifetime considering the development and growth of digital life and interaction the probability of data breaches affecting an individual, and therefore the probability of linkability raises. Furthermore, taking the assumption of Moore's law into account to which microchip complexity doubles every two years, future computational powers will keep increasing exponentially and facilitate linking of data. Therefore data controllers and data processors should make transparent for data subjects, under which conditions personal data will be or actually are linked (for example within privacy policies). This is necessary to make the transferral of data across contexts transparent for the data subject.

Transp-Req: Data controllers and data processors should make transparent for data subjects, under which conditions (potentially) personal data may be, will be or actually are linked.

4.1.6 Privacy and security breach notification

Data breaches that affect an individual as well as the possibility of linkability need to be prevented. It has to be in the control of the data subject to decide where linkability is allowed or even required. It has to be transparent for data subjects where linkability is possible or already conducted. Therefore data controllers and processors should inform data subjects and supervisory authorities timely on privacy and security breaches and give advice on how to cope with the consequences.

Transp-Req: Data controllers and data processors should inform data subjects concerned and supervisory authorities timely on privacy and security breaches and give advice on how to cope with the (potential) consequences.

4.2 Decreasing the risks to Privacy4Life by data minimisation

For most of the data subjects it is not clear or they are even not aware which data about his/her behaviour are particularly stored and how long the duration of this storage is. This is also a question of transparency and in this case these two principles are closely related to each other.

4.2.1 Minimal quantity and sensitiveness

To guarantee storage of minimal quantity of personal data, it is absolutely necessary to inform the data subject about personal data stored and in particular about the use of these personal data. Mostly collected data of a data subject are used for profiling and for data mining. Service providers want to offer their service in the best way to their customers and therefore use profiling to offer specific goods to the user. This customer care mostly also comprises specific offers to a user of the service. Many users do appreciate these offers. But they do not know the data mining behind. There is no transparency about which data are stored and used for profiling and for how long they are stored. In many cases the privacy policy of the service provider does not even mention the fact of profiling or data mining or the customer does not have the chance to use the service and not to be targeted. In conclusion it is necessary that the data subject can decide if he wants to get extra, "personal" offers and therefore is part of the profiling system, or not.

DatMin-Req: Data controllers and data processors, and system developers should minimise the storage of (potentially) personal and sensitive data as far as possible.

Furthermore, most of the service providers do not sufficiently differentiate data they are collecting. It may happen that many sensitive personal data are collected, processed and used for

data mining even if the regulations of the Directive determines special provisions for the collecting and processing of sensitive personal data. Also here the data subject is often not aware that these data are collected, stored, processed and used for data mining.

DatMin-Req: Supervisory authorities and privacy organisations should support individuals, data controllers and data processors, and system developers to fulfil the principle of data minimisation by giving advice concerning concepts and implementations, pointing to best practices and support research and development in this field. This may be done by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible.

4.2.2 Minimal timeframe

Regarding the lifelong aspect, it is often not adhered to the minimal timeframe for the storage of personal data. The data subject needs to get the control about the timeframe of storing of personal data. Therefore, the timeframe of storage and use of potentially personal data has to be minimised as much as possible and there has to be transparency for the data subject. If there is no legal basis for the use, data should be fully erased.

DatMin-Req: Data controllers and data processors, and system developers should minimise the timeframe of storage and use of (potentially) personal data as far as possible. After that time, the data should be fully erased. This should comprise temporary files or data which have been distributed to other media or recipients as far as possible.

4.2.3 Minimal disclosure

Disclosure of information constitutes one of the key prerequisites for user control through self-determination, which is a core principle for privacy-enhancing identity management systems. Establishing user control creates satisfactory interactions, human well being, and diverse relations. Other important social aspects of this requirement are: consciousness (individuals have to be aware when their data is processed), comprehension (they need to understand what is actually happening when data is being collected) and consistency (data subjects need to be able to anticipate to the changes of people, preferences, and situations).

DatMin-Req: Data controllers, data processors as well as individuals should minimise the disclosure of (potentially) personal data as far as possible.

4.2.4 Right of access

Regarding the reference to lifelong aspects, it can be reverted to requirements on access control policies. This requirement demands for an option for access control policies to expire after an amount of time. Access control policies should support conditions and reasoning about time. Time can impact the validity of certain conditions in the policies to be used to support policies that might be valid up to some time or after some time (for example, embargo on data, data that become public after a given time or data that should be deleted after a given time).

With reference to the general requirement of data minimisation, the policy language should support and encourage minimisation of the amount of personal information that is revealed in order to gain access to a resource. The architecture should definitely not assume that all information about the subject is readily available when the access decision is made. Rather, the list

of attributes that need to be revealed, or the predicate that needs to be proved, should be explicitly specified by the server, or perhaps even be the result of a negotiation between the client and the server. The client should then have the option to reveal only those attributes that are strictly necessary. This requirement encourages the basic requirement of data minimisation and helps the data subject to control the digital footprint over lifetime.

It corresponds to Art. 6 of the Directive [Euro95, Art. 6], stating that personal data shall not be kept for longer than necessary for the purposes for which the data was collected. After achieving the purpose for which the data was gathered, it has to be erased or rendered anonymous.

4.2.5 Minimal correlation possibilities – limiting linkability

To protect the data subjects, they should have the possibility to decide whether partial identities can be linked to control her partial identities over lifetime.

DatMin-Req: Data controllers and data processors, and system developers should minimise linkability and linkage of (potentially) personal data as far as possible.

Furthermore, most of the service providers do not handle context separation. In contrary, most of the contexts are linked to get even more information about the data subject and her behaviour. In general contexts have to be separated regarding the lifelong aspect, especially when connecting them is not necessary for the aim of the formal identity.

DatMin-Req: Data controllers and data processors, and system developers should minimise multi-purpose or context-spanning use of (potentially) personal data as far as possible. They should provide mechanisms for context separation of these data.

It appears that for instance in the Netherlands, one unique identifier was used in different contexts. The use of such a unique identifier should be prevented. The individual should be able to use a range of identifiers with varying degrees of observability and linkability. This means data subjects must have a choice to operate anonymously, pseudonymously or known. They should also be able to use identities provided by public bodies or enterprises, as well as ones created by themselves, to be able to provide certainty about their identity to other entities and therefore promote accountability when required.

DatMin-Req: Data controllers and data processors, and system developers should avoid the use of unique identifiers which may be used in different contexts. They should use diverse identifiers where possible.

Furthermore, the requirement regarding anonymous and/or pseudonymous access control is significant. Thereafter a data subject shall have the possibility to access a resource in an anonymous or pseudonymous way. For an anonymous access, the server makes sure that the user fulfils the necessary requirements, for example, “age > 18”, while the required attributes allow the user to stay anonymous. This is of course only possible if (1) the required attributes (like “age > 18”) are applicable to a big number of people and the data subject can therefore not be identified, and (2) the underlying technology supports proving of the attributes in an anonymous way.

Anonymous and/or pseudonymous access control is important for the data subject’s control of his personal digital footprint and for the lifelong data control. It gives the opportunity to access a resource without disclosing personal data and without the assignment of the clickstream and thereby extend the digital footprint.

DatMin-Req: Data controllers and data processors, and system developers should support anonymous or pseudonymous authorisation and access control of users where possible.

4.2.6 Avoid or limit irrevocable consequences

If within a process it appears, that something may have irrevocable consequences for the privacy of data subjects, it has to be ensured that either the data subject has the choice to decide or these consequences should be minimised in general.

DatMin-Req: Data controllers and data processors, and system developers should minimise irrevocable consequences concerning the privacy of data subjects.

4.2.7 No coupling to consent

Some Member States have special regulations regarding the coupling of consent or a general principle of only using data for its original purpose (for example, the German § 12 Abs. 3 TMG, wich stipulates, that the use of uer data for purposes other than providint the service or advertising or passing on the data to another firm requires express consent of the data subject. In doing so, the data controller may not make provision of the search service tependent on the consent to use for other purposes if the user has no other access or reasonable access to such telemedia.). Therefore "coupling" of data is prohibited.

DatMin-Req: For societally relevant services which may be accessed in an anonymous or pseudonymous way, data controllers and data processors should not make the rendering of services contingent upon the consent of the user to the processing or use of her data for other purposes if other access to these services is, not or not reasonably, provided to the user.

4.3 Fair use – Controllable and controlled data processing

For the controllability of the full lifecycle of a data subject major challenge lies in the control of information that is revealed or published by others than the data subject. In this respect, it is important to notice that others can be individuals as well as companies or institutions. From a legal perspective, this topic is covered in the Lindqvist case; the European Court of Human Rights decided that it is not allowed to publish personal data of others on a website without their consent. The court decision can be applied to all forms of publishing personal data, although the Internet environment will be most relevant. Even though the subject seems legally covered, this remains dependent on awareness of individuals and, for that reason, will mainly remain as an ex-post measure of enforcement. Trying to inform concerned individuals before information about them is published would possibly imply that a database is needed of all individuals and their personal details in order to facilitate this. That is not the most desirable solution.

Other difficulties arise in the context where data can be indicated as (personal) data about more than one person, like for instance relationships or medical data about hereditary diseases. Does the fact that data reveal something about oneself as well as about another individual imply that disclosure is prohibited, unless there is consent of the other data subject? That might be problematic in specific cases where the disclosure of these data might be required in order to enable accurate decision taking, in particular with medical data, even though the disclosure of a hereditary disease to one's children might conflict with the right not to know. And, of course, gossiping would become prohibited. Solutions may be found in the technical domain. For

instance, it may be technically enforced that before posting or publishing content, the consent of all individuals concerned have been obtained.[13]

4.3.1 Purpose binding

With regard to purpose limitation, the data controller has first of all to inform the data subject of the purposes for which data are being collected.

Control-Req: Data controllers and data processors should restrict the processing of (potentially) personal data to a predefined purpose.

Control-Req: Data controllers and data processors should be specific in the definition of the respective purposes.

Often the problem rises that purposes are interpreted different by the controller and the user. To avoid this problem, purposes have to be described and privacy policies to be defined in a clear and understandable way. But often purposes are defined inexplicitly because the controller does not want to be tied to clear purposes to have the opportunity to use data for different purposes. In some cases the definition of processes may change. This also leads to a change of purposes and therefore a new consent or new legal basis for the processing is necessary. The data subject has to be informed and perhaps a new consent should be given. But it has to be kept in mind, that the processing still needs to be feasible for the data controller and the requirement should not lead to the situation that the data controller needs to ask for consent before every processing.

4.3.2 Accountability

When taking into account that technical development can increase the information value of current data, accountability for data processing becomes a specific point of attention. The protection of data and carefully considering the disclosure and sharing of data are key aspects. If processing of personal databases on a legal basis or consent, the data processor is also accountable for the processing. Within a company there have to be clear definitions on who is responsible for processing and storage of or access to personal data. Data controllers have the responsibility to adequately protect the data in their systems and the use of personal data is bound to certain legal requirements, such as the requirement of an indicated purpose. When a database is used by the controller, clear concepts regarding deletion or other obligations already need to exist.

Control-Req: If the data processing is based on consent: Data controllers should limit the data subject's consent in time by default.

Control-Req: If the data processing is based on consent: Data controllers should ensure that the data subject can withdraw the consent without unexpected impacts on his privacy (because of irrevocable consequences).

[13] Note that we do not discuss here individuals in the role of a public figure, i.e., a celebrity or otherwise famous person whose actions are the focus of public interest. For public figures, the public's right to be informed by the press may dominate their right to privacy – at least in those contexts of life which are related to their celebrity.

Control-Req: Data controllers and data processors should ensure that the parties processing the data are accountable. This includes the definition and assignment of clear responsibilities.

Control-Req: Data controllers and data processors should prohibit identity theft, especially in situations which may have privacy-infringing impacts

4.3.3 Organisation of data processing and possible conflicts

Collecting, processing and deletion of personal data within a company have to be defined in detail beforehand and has to cover the full lifecycle of personal data.

With regard to deletion of personal (sensitive) data, controllers and processors have to be aware of the fact that there have to be regulations on deletion when a new database or profile is created or personal data are collected. There have to be clear regulations and processes on when and how personal data have to be deleted if there is no legal basis for processing or no purpose left. There furthermore could be mechanisms to regularly control the legal basis for the processing of personal data and in consequence the deletion if personal data are not necessary any more. In addition controllers and processors need to be aware that conclusion of a contract should not be connected to the data subject's consent in the processing for marketing purposes.

Control-Req: Data controllers and data processors should conceptualise and plan their privacy-relevant data processing beforehand, thereby covering the full lifecycle of data (from creation to deletion). This comprises to plan the process and set the conditions for potential or factual linkage of data and – if the data processing is based on consent – also for its revocation.

Control-Req: If identifiers are created, data controllers and data processors should already foresee concepts and procedures for their erasure after the usage period.

Control-Req: Data controllers and data processors should also plan for emergency situations (for example, privacy and security breaches).

The Internet is more and more used by natural persons to publish information not only about themselves, but also about others. Therefore often information about third persons is processed without the consent and even knowledge of the persons concerned. Especially within social networks, photos of friends are uploaded. Even if all people on the picture agree to its publication, they may not like being public some time later. More and more of the contents on the Internet are edited by private persons, through social networking services, such as FaceBook, "blogging" or "twittering". It is a legal challenge to clarify the question regarding the enforcement of privacy rights of users that act as data controllers when publishing personal data about others on the Internet and whether this activity is subject to data protection law and what the consequences are [Korf09]. In general, the Directive [Euro95] does not impose the duties of a data controller or an individual who processes personal data "in the course of a purely personal or household activity" (household exemption). It is a legal challenge to clarify the question regarding the enforcement of privacy rights of users that act as data controllers when publishing personal data about others on the Internet and whether this activity is subject to data protection law and what the consequences

are [Korf09]. This question is discussed within the Working Paper 163, Opinion 5/2009 on online social networking of the Article 29 Data Protection Working Party [Arti09b, p. 5 ff.] and states that in most cases, users are considered to be data subjects.

But some activities of a user of a SNS may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller (for example, when the social network is used as a collaboration platform for an association or company) [Arti09b, p. 5 ff.]. In these circumstances, the user needs the consent of the persons concerned or a legal basis for the processing of personal data. The directive furthermore states, that also a high number of contacts in a social network "could be an indication that the household exception does not apply and therefore the user would be considered as a data controller" [Arti09b, p. 6]. This shows that the Art. 29 Working Party inclines to make users who uploaded content to a wide audience responsible as data controllers. In conclusion it can be said that users of social network sites or blogs, uploading materials for the dissemination to "an unrestricted number of people" are not covered by the household exemption [Korf09].

Most of the users are not aware of the fact and the related duties. They need to learn and need to get information when acting within the web or especially SNS. Therefore there should be guidelines for the user for acting in conformity with the law as well as from the other perspective on how to contact a data controller and how to exercise the rights under the Directive.

Self-determination and controllability of personal data does also relate to portability of data. This may mean that the data subject can control her personal data in a way that they are portable within the web. For example there could be mechanisms that make personal data in a profile of a social network compatible to another social network. In this case the user could "move" one profile to another social network if she wants. This could either be after quitting the participation in one social network and implementing the profile into a new social network or even having identical profiles in different social networks without creating it completely new within the registration process. Profiles could also be exported to the local system of the user (for example, for archiving). It is an important feature for Privacy4Life to preventing "lock-in" situations, i.e., if the user is factually dependent on the data controller (for example, the social network) and cannot leave even if she does not agree with the privacy policy in place.

Control-Req: Data controllers should prevent lock-in situations. For example, SNS providers should provide portability for user profiles.

Joint responsibility of personal data raises the risk that the data subject loses control about her personal data. Therefore it is necessary to clearly define responsibilities in case of joint responsibility.

Contrtol-Req: Data controllers, and in SNS also peers, should clearly define responsibilities in case of joint responsibility of data as well as the rules for jointly or separately using the joint data (for example, in a (privacy) policy or another binding contract).

4.3.4 Sensitive data

With regard to the general principle of transparency, the data subject should have technically and legally the opportunity to control her sensitive data (cf. Section 2.2) that accumulate within information systems or in databases. This may work by claiming the right of erasure [Euro95, Art. 12] by the data subject.

Control-Req: Data controllers and data processors should be extra cautious with (potentially) sensitive data.

To exercise the right of erasure, the data subject needs to know which personal data are stored in which databases or information systems. Therefore digital footprints and especially the collecting, processing and storage of sensitive personal data have to be transparent for the data subject. This is required to avoid the possibility of linkage of sensitive data. Even if the data subject uses a pseudonym, it should be under her control which data are related to the pseudonym. The data subject needs to have the possibility to decide whether the pseudonym contains too many personal (in this case sensitive) data and maybe in the consequence deletes the whole footprint or even parts of the pseudonym. It should also be under the data subject's control to decide, for example, that data with a certain age are not allowed to be related to the digital footprint (of a person or a pseudonym).

Biometric data can also be defined as sensitive data. The European Union's independent advisory council for data protection issues, the so-called Art. 29 Working Party, comments on the sensitive character of biometric data [Arti03, p. 10]. Biometric identifiers are by definition non-revocable, which needs to be considered with regard to the lifelong aspect. Biometric data cannot be changed, once it has been recorded. Static biometric identifiers that do not change over lifetime are particularly critical. If more applications use authentication or profiling based on static biometric identifiers, the risk of unauthorised use of and access to biometric data exists during the remaining lifetime of an individual. Note that more privacy-friendly biometrics are being proposed which prevent re-use of biometrics in a different context, e.g., by only employing dynamic biometric identifiers that won't be released uncautiously (like speaking a specific password) or by clever encryption technologies (like biometric encryption[14] or revocable biometrics[15]).

However, often biometric data are translated to code and this code is used to identify or authorise a person. Identification of the person and direct use of the biometric identifier are not necessary in this case. Just like all other digital data, the data can be changed or revoked then. Therefore, transparency of processing of biometric data has to be ensured and there has to be the obligation to notify the data subject in case of loss or stolen biometric data.

Fallback solutions need to be in place addressing a process for individuals who cannot enrol or whose biometric data was compromised. Also fallback solutions for alternative means of access to the service should be provided, especially if biometric solutions are even more widely used and people may be hampered from access to certain services or entering certain locations.

There is also a large number of sensitive data that are not explicitly defined in Art. 8 of the Data Protection Directive. Some Member States have taken the opportunity allowed under Art. 8 of the Data Protection Directive to expand the definition of sensitive data also to data relating to offences, criminal convictions or security measures.[16] There might also be some cultural differences regarding the definitions of sensitive data within the Member States which might lead to the fact, that sensitive data are defined in different cultural ways. Therefore all Member States have to clearly define the definition of sensitive data and have to implement the provisions of the Data Protection Directive in their legislation.

---

[14] See, e.g., C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. K. V. Kumar: Biometric Encryption™, Chapter 22 in R. K. Nichols (ed.): ICSA Guide to Cryptography, McGraw-Hill, 1999, http://www.catcard.arizona.edu/bca/Biometric_Encryption.pdf.

[15] See work in the FP7 project "TURBINE – TrUsted Revocable Biometric IdeNtitiEs", http://www.turbine-project.eu/.

[16] For example, Italy (Italian Data Protection Act, Art. 24) or Finland (Personal Data Act, § 11).

4.3.5 Data subject rights

Apart from the data subject's rights stipulated under the provision of the Directives [Euro95 and Euro02], one might think of data subject´s rights that are not yet statutorily regulated. For example, it would be useful in many situations to have a "right to start over". The data subject undergoes different phases of life that comprise different kind of personal data. Mostly, the risk of processing personal data is minimised beforehand by legal regulations or technical measures. But in some situations it is not possible to cover all risks and subsequently user control of the processing of his personal data is not possible. This might be the case if wrong personal data are used without one's fault (for example, governmental or third party fault). This incorrect information may cause various problems for the data subject in the daily life and the data subject may furthermore seek for rehabilitation (for example, if wrong personal data appear in web search engines) when the incorrect information puts the person in the pillory.

Therefore the data subject needs to have the "right to start over" in certain situations and should furthermore have the possibility of rehabilitation.

In a lifelong context it becomes even more difficult to keep track of what others (might) know about an individual. The data subject has no possibility to make it comprehensible what others may know or what kind of personal data someone else has. The problem that rises in this context is the handling and organisation of the massive amount of data in case of supporting the user in keeping track. There is also no approach on how to make such data accessible or what kind of interfaces could be used. The data subject does not have any solution how to deal with outdated file formats or hardware components, regular backups and technical updates of his track application. As all these questions still remain unresolved, it is also unclear if additional legal regulations are needed especially with regard to prevent the abuse of data track information by spying or by others unlawfully asking for access to this information.

For the data subject it is necessary to also be informed who has obtained certain personal data, for example, data from the electronic personal eID or the electronic health insurance card and where processing of personal data occurs. Therefore the data controller should offer an information system for the user to create transparency on where and what kind of data were processed to whom. Data controllers should make this information available for the user and readable with common systems (for example, a list containing who has asked for what kind of data of the electronic health insurance card and for what purposes or a token that may read and tell the user who has the bank account number or the date of birth).

Control-Req: Data controllers should provide the appropriate information to the data subject to create transparency of what kind of privacy-relevant data is processed by whom. Further they should support data subjects in exercising their rights, e.g., by lowering the threshold to get access to personal data via online solutions.

The data subject does not have full overview over personal data that exist and that are part of the digital footprint. In this context it is also important that with regard to the digital footprint data as total may be personal, even if some data within the digital footprint may not be personal. This means, that data that are not qualified as personal data as such are part of the footprint and in the context of the footprint they are qualified as personal data because they refer to an indirectly identifiable individual. Even if there is no identification with the name or address or social security number, the footprint is identification based on the possibility to single out an individual. For this reason it is even more important for the data subject to be informed about the digital footprint.

4.4 Delegation in identity management

In the context of identity management throughout life, one focus lies on investigating the necessity of delegation for people who are not able to manage their needs of privacy for a limited time or forever. This section describes the general and existing concepts of delegation and derives requirements for delegation in identity management:

Delegate-Req: Data controllers, data processors, and system developers should foresee that data subjects can delegate their identity management to proxies.

Delegate-Req: Data controllers, data processors, and system developers should enable delegation of identity management limited to specific proxies and specific scopes (such as purposes, applications, data controllers, time etc.).

Delegate-Req: Data controllers, data processors, and system developers should enable revocation of delegation of identity management under defined conditions.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for a data subject to get an overview of decisions by her proxy regarding processing of personal data.

Delegate-Req: Data controllers, data processors, and system developers should provide concepts and mechanisms for identity management after one's death.

In the following it will be differentiated between the common terms of delegation, as defined above and as legally defined and the definition which is more under the civil law aspect, namely delegation based on explicit decision/will of the data subject. As in the common term of delegation this is mostly a stage of life in which the data subject is not capable to exercise her rights, delegation based on explicit decision/will of the data subject refers to stages of life in which the data subject explicitly wants to transfer full or partial legal authority of representation to another individual.

4.4.1 Delegation based on legal provisions

As mentioned above, the data subject needs to be represented by another natural person who exercises the right on behalf of the data subject concerned during certain phases of life. This may start when a child is born and it may continue in case of adults that may have temporary or permanent needs to get support, and it may finally end with the dead of the data subject‘s last will. Each stage has significant question on how to handle identity management and in particular personal data and therefore has different requirements. It is quite clear, that a baby is physically less able than a 10 year old to interact with technical devices. But at least small children are not able to decide on their own which data are created and processed and how their private sphere can be controlled. Fundamental law does not explicitly allow for representation by others. Fundamental rights are by nature non-transferable, personal rights.

Relating to stages of life and the handling of one's private sphere furthermore raises the question if the above mentioned legal regulations are sufficient for the data subject to also exercise the right of informational self-determination. In some legal delegations, for example, in case of a contract,

the proxy has to process personal data of the individual represented (e.g., in Germany § 28 I BDSG Bundesdatenschutzgesetz). This case is legally correct under the civil law, but also has consequences for the fundamental right of informational self-determination what leads to the question if fundamental rights are transferable to a proxy in general. This may be a problem with personal fundamental rights. The right of informational self-determination may be defined as such in some cases and raises the question if personal fundamental rights are transferable in general. If the answer is positive, it may be necessary to find new legal regulations or instruments that stipulate the intercourse with such cases. This also leads to the fact that providers have to supply appropriate technical infrastructures on a legal basis.

Therefore delegation in privacy issues should be recognised by law as far as legally possible, for example, requiring actions in person only where private law acknowledges similar requirements (like the requirement that a will cannot be made by a proxy could correspond with a regulation that privacy rights for the post-mortal period require a specific mandate). It must be compulsory for data controllers to accept declarations of the proxy.

The above mentioned definition of delegation can be derived from this analysis.[17] Delegation furthermore means the transfer of power of legal representation of one natural person to another natural person. This transfer of power can either result from provisions which lay down legal prerequisites or from the concerned natural person's decision. The delegation of exercising fundamental rights on behalf of the bearer of the fundamental right is as such not known in current legal frameworks as fundamental rights are non-transferable personal rights. Legal representation does however impact fundamental rights as a secondary effect.

Mapping delegation technologically a number of requirements can be derived:

Usually delegation is expressed by issuance of a credential (“mandate”, attribute certificate) to the proxy. Among the important procedures to be specified are: issuance of the mandate to the proxy, invocation of actions under the name of the principal with the mandate, verification of the mandate, revocation of the mandate from the proxy and expression of acceptance of the mandate by the proxy [PSCP08].

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for issuance of the mandate of the proxy, invocation of actions under the name of the principal with the mandate, verification of the mandate, revocation of the mandate from the proxy and expression of acceptance of the mandate by the proxy.

Delegation has to be enabled without transferring the original credentials (such as tokens or certificates) of the principal to prevent identity theft. Possible implementations include derived credentials for proxies or that the proxy uses own credentials to get access and then indicates that s/he acts on behalf of the principal.

Delegate-Req: Data controllers, data processors, and system developers should support derived credentials for proxies or that enable the proxy to use own credentials to get access and to act on behalf of the principal.

Actions taken by a proxy must be traceable for the principal, for example, by writing into the data track of the principal or granting the principal a right to access the relevant information in the proxy’s data track. Also the data track of the proxy should indicate the fact of having acted as proxy and which data was released. However, in case of minors, as principals the logging requirements must not overstrain the capabilities of average parents.

[17] See above, Section 2.1.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms that allow the principal to trace actions taken by the proxy.

The principal must be able to declare preferences and conditions to the power of proxy, for example, to partially or absolutely restrict certain disclosures, to stipulate preferences or by giving a general guideline for data usage inform of preferences but allowing an exception for a certain transaction s/he is interested in regardless of the data required.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for the principle to declare preferences and conditions to the power of the proxy.

The proxy's own desires for maintaining her privacy have to be considered in addition to the privacy requirements of the principal. Data minimising solutions, for example, by anonymous authorisations, can help preserving the privacy spheres of both parties involved.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms to maintain the proxy's private sphere

The following subsections exemplarily analyse some stages of life in order to show how the management of one's private sphere with respect to handling her privacy may work.

4.4.1.1 Fruit of the womb

Privacy throughout life comprises a very early stage of life, the prenatal phase of an individual. Even in this stage of life there might be the need to protect personal data, for example, considering the privacy implications of prenatal DNA tests. In many EU Member States there are discussions about the issue of genetic analysis and the threat of using genetic data poses for individual's right of informational self-determination as well as potential discrimination. Regulations regarding requirements for genetic analysis and the use of genetic data could be a solution.

4.4.1.2 Children and teenagers

Growing autonomy is an important issue in protection of children's rights, in any area of law. The complexity of situations involving minors is based on the fact that children, despite having full rights, need a representative to exercise these rights – including their privacy rights.

Data protection for children starts within the first days after birth and the processing and storage of birth data or medicine data within the hospital. The protection of personal data of children resides more or less in the responsibility of parents or legal guardians. But when a child grows up, other responsible persons for data processing in different areas of life may become involved, such as teachers, doctors or supervisors [HaPS08].

The rights of the child, and the exercise of those rights – including that of data protection, should be expressed in a way which recognises both of these aspects of the situation [Arti08]. Until a certain age children have no way to monitor data processing, simply because they are too young to be involved in certain activities. If their parents decide, for example, to put the child's pictures on their profile in a social network, it is the parents who make the decision about the processing of their children's data and give the consent to do so on behalf of the child. Normally, putting pictures of another person in a social network profile requires consent of that person, the data subject. In the situation described here, the parents are entitled to express the consent in the name of the child. Such situation may put the parents in the double role – of data controllers while publishing their child's personal information open on the web, and, at the same time, of consent issuers as the child's representatives. This double role may easily lead to conflicts. Parents must take great care not to cross the line of the child's best interest when processing the child's data.

It is necessary for the parents or other representatives to listen carefully to the interests of the child at least beginning from a certain age and consider those interests when making a privacy-relevant decision as that decision is binding for the child [Arti08]. When the child reaches legal age, it may want to change the recent decision of the parents. Therefore the child needs to know what decisions about processing of personal data were made by the representatives. Afterwards the child needs to give her explicit consent for the processing of personal data. This may be implemented in certain operations in a way that the operator is reminded that the person is over 18 and now the explicit consent is needed. This is relevant in many circumstances, for example, medical matters, recreational activities of the child, school matters, or agreements made by the parents before the child's majority.

As children and teenagers are in the process of developing physically and mentally, the rights of the child and the exercise of those rights – including the rights of data protection– should be accomplished in a way which recognises these aspects of the situation. Especially the adaptation of the degree of maturity of children and teenagers is a central aspect that has to be taken into account by their parents. Children gradually become capable of contributing to decisions made about them. It is natural that the level of comprehension is not the same in case of a 7-year-old child and a 15-year-old teenager.[18] This, in particular has to be recognised by the children's representatives. Therefore the children should be consulted more regularly by adults, teachers or care-takers about the exercise of their rights, including those related to data protection.

The children's representatives should also think about a way to document privacy-relevant decisions so that the children or young adults can later easily understand what personal data have been disclosed to whom and under which conditions. They also may then choose to actively approach certain data controllers to give or revoke consent concerning data processing or to request access, rectification or erasure of their personal data.

4.4.1.3 Adults lacking privacy management capabilities

For adults that may have temporary or permanent needs to get support or that others act on behalf concerning decisions on their private sphere, we distinguish between delegation for legally relevant actions and non-legally relevant actions. All legally relevant actions regarding processing of personal data are based on national legal regulations such as delegation or legal guardianship.

In case of non-legally relevant actions, such as help with a social network or the Internet in general the person concerned can freely decide what to do. The principal could choose a proxy (for example, a care-taker) to act in the name of the person on the basis of a contract to manage the private sphere. Then the person concerned should clearly define her expectations and needs regarding the representation and the power of disposal.

4.4.1.4 Deceased people

In situations where a person has deceased, the instrument of law of succession applies. The European Data Protection Directive 95/46/EC assigns the right of privacy and data protection to "natural persons" (Article 1). Deceased persons are no longer regarded as data subjects. Protection against an unregulated processing of data concerning deceased individuals in some European legal

[18] The level of comprehension is defined in different ways. For instance the US-American Children's Online Privacy Protection Act (COPPA, Title XII – Children's online privacy protection, SEC. 1302) defines a child as an individual under the age of 13.

frameworks[19] is provided by means of a "post-mortal personality right". In some situations, the instrument offered by the law of succession might not be sufficient – further regulations are needed.

For instance, some users of social networks want their profile to exist even after death or at least would like to be informed how the provider handles the personal data and the profile after death. Here the action of providers of social networks is required to find mechanisms and concepts for the handling of profiles after death of the user. Various mechanisms are thinkable, for example, the user could determine how her profile should be handled after death within the registration process (deletion, blocking, proxy to contact, etc.). Therefore, SNS providers need to define clear measures and concepts to determine the handling of profiles after one's death. In some situations even the autonomous action of the SNS provider might be essential for the protection of users. For example if a SNS user dies and the press accesses the SNS site to copy pictures, contacts, etc. of the dead user, the provider has to balance the protection of the users rights and her competence to, for example, block the profile without the consent of the legal assignee (because this has to happen very quickly).

Meanwhile new services appear on the market which offer to send out secure messages to friends after the death of the user. Their goal is to give people a safe way to share account passwords, wills and other information. When users book the service against payment of a fee, they get options for when to send messages or to delete some messages permanently after their death. It is problematic if authentication credentials of the user have to be transferred to the service which opens the way to misuse because it is not distinguishable for others whether the user or the service acts.

Delegate-Req: Data controllers should define how to deal with the data subject's data after her death. In particular, SNS providers should define and provide mechanisms for the user to determine the handling of profiles after her death.

4.4.2 Delegation based on explicit decision/will of the data subject

The civil law knows the instrument of legal representation also for cases where the concerned individual is fully in possession of his/her mental capabilities and decides on his own to transfer the exertion of rights to another person (for example, Articles 172 et seq. German Civil Code[20]). Various reasons exist why a data subject may wish to transfer the full or partial legal authority of representation to another individual. For example a person may simply be unavailable for a longer period of time with no access to information technology which would allow transmitting and enforcing remote decisions (for example, during a scientific or recreational journey to a secluded region). Or a data subject may feel that certain services which are handled online are better to be understood by friends or even a professional data custodian. Actions of and decisions by the authorised representative may have consequences also for the fundamental rights of the principal who at first glance delegated, for example, only the authority to the agent to close one contract on his behalf. Delivering the contractual duties however will possibly also require the processing of personal data. The legal authority to represent a principal in closing a contract does include the implied authority to initiate the data processing steps necessary to fulfil the primary goal. The instrument of legal representation based on the data subjects declared intention may also have effect after the data subject's death. The data subject may during his/her lifetime lay down a last

[19] Such as Germany: so-called "Mephisto decision" of the German Constitutional Court; BVerfGE 30, 173.

[20] English translation of Bürgerliches Gesetzbuch: (German Civil Code): http://bundesrecht.juris.de/englisch_bgb/englisch_bgb.html.

will which binds the heirs. This last will may also comprise decisions regarding how to treat documents or electronic files containing personal data.

The Art. 29 WP defined in its Option 2/2009 [Arti09a] principles regarding exercising the right of children. These principles may also be helpful for determining principles on delegation in general, because proxies may have the problem that delegation in privacy relevant situations might be interpreted in different ways. This means that one may have different needs on good practice of handling privacy.

4.5 Practicability of mechanisms

Mechanisms for Privacy4Life, and in particular those being integrated in identity management systems, can only help individuals if they are easy to apply. The following requirements primarily address data controllers as those are the responsible parties concerning data processing. However, the requirements should be seen as guidance for developers of mechanisms even if they are not involved in the daily operating of the ICT systems. Note that it is not required that all mechanisms work in the online world, but there may be workflows for identity management which do not use computers at all.

Mech-Req: Data controllers, data processors, and system developers should develop, provide and use the appropriate IdM mechanisms for all parties involved in privacy-relevant data processing.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are accessible.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are effective, i.e., having the desired impact within a reasonable time frame with a reasonable effort.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are transparent concerning their potential impacts, limitations and side-effects.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are transparent concerning their effective impacts, limitations and side-effects.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are usable for the specific user group (for example, by well comprehensible user interfaces, limitation in complexity etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the devices bearing the IdM mechanisms have an appropriate security level (including hardware, operating system, software etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the management of (potentially) personal data has an appropriate security level concerning long-term storage, backup and recovery.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the appropriate IdM mechanisms will also work in a – due to long-term effects – potentially changed environment and prohibit lock-in risks (for example, by migration strategies, ensuring long-term portability where needed etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, there are fallback solutions in case the appropriate IdM mechanisms fail or are not accessible.

4.6 Conclusion

This chapter shows that in selected situations analysed above, concrete technical and legal requirements can be derived. These requirements impact different and sometimes also multiple actors that may implement the requirements within their systems. In many situations there is still much to be done to improve identity management throughout one's whole life; the implementation of requirement, and therefore the improvement of identity management is mostly aligned to the interest of the actors involved. Therefore law makers and technical developers need to cooperate to not only adjust, but furthermore enforce the above mentioned general principles.

Chapter 5

Tools and mechanisms for Privacy4Life

This chapter focuses on technological issues with respect to Privacy4Life. As the value of privacy-enhancing technologies becomes more and more accepted (cf. [Comm07]) and user-controlled identity management systems have been proposed to solve the challenges of maintaining one's privacy [LeSH07], applying these concepts to Privacy4Life seems to be promising. However, this is easier said than done as we argue in Section 5.1 with preliminary remarks. Section 5.2 sketches requirements for user-controlled identity management systems to maintain lifelong privacy. Basic building blocks for that exist in principle as it is shown in Section 5.3 which lists important technical primitives and tools. It also analyses long-term issues of these primitives and tools which would have to be considered when employing them in user-controlled identity management systems. This analysis yields further requirements to technical concepts and solutions which are depicted in Section 5.4. Finally Section 5.5 summarises the results.

5.1 Preliminary remarks from a technological perspective

Over the past five decades, tremendous advances in information and communication technologies have substantially facilitated to collect, store, combine, and process information. Whenever such information relates to human beings, data processing affects the informational privacy of the respective persons. So advances in technology are the root cause of many privacy problems our information society is facing today.

However, interference with people's privacy does not necessarily stand in a direct relationship to the level of technological development, but it more depends on the actual design of systems, protocols, and infrastructures. This latitude has fueled the idea to cure the problems created by technology with more technology, as first mentioned by Paul Baran [Bara65] in the 1960s. Nowadays, the term privacy-enhancing technologies (PETs) refers to technical building blocks for systems that are designed to avoid privacy problems without constraining the system's functionality unnecessarily [GoWB97]. So ideally, privacy-enhancing technologies should help people to extract all benefits from technological advances without experiencing the negative side-effects on their privacy and individual freedom.

This sounds too much like a panacea, so it is appropriate to ask how much we can expect from privacy-enhancing technologies in general; and in particular when we consider privacy throughout life.

Computing technology became available to governments in the 1940s, to large enterprises in the 1960s, and to end users in the 1980s. Since then, the field has changed very rapidly: typical depreciation periods range from three years for hardware to about five years for software. Maintenance of legacy systems turned out to be very cumbersome and costly. So effectively, even experts lack solid experience with large systems running for more than two decades. Moreover, the existing experience with long-running systems is almost exclusively drawn from closed architectures, physically shielded from the outside world and administered by professionals. So it cannot be generalised to security technology for open distributed networks, which are exposed to a much wider range of threats. Here, the typical latency between the release of the latest patch and the next successful break is usually counted in days (sometimes hours). Hence, looking ahead, it is unrealistic to expect that consumer security technology will reliably protect people's privacy in common computer-mediated social interactions over a lifetime. This statement will probably remain valid in the foreseeable future, unless major scientific discoveries substantially change our conception of computation and information.

Moreover, even if perfectly secure privacy-enhancing technologies existed, its security would be bounded by the weakest link: the user. It is unrealistic to assume that average citizens are always capable to use privacy-enhancing technologies in their own interest without making serious (and irrevocable) mistakes [AcGr05].

Taking both limiting factors together, the prospects for a long-term privacy-friendly information society by technology are very dim. Carrying the matter to the extremes, two pure strategies for a society to deal with this situation come to mind:

1. Turn back the clock, abolish freely programmable computing devices (or substantially limit access to them) and provide only ICT systems with limited functionality where compliance with data protection law is enforced, or
2. give up claims for (long-term) privacy in large parts of social interactions.

The first option is so unrealistic that nobody discusses it seriously – and there would be several drawbacks, too. The second option does not square well with normative notions of privacy as a fundamental right and it may impose social costs in the long run. Although difficult to quantify, these costs include lost freedom, fewer innovation through conformity, reduced competition, and possibly resource misallocation due to overt discrimination. So none of the pure strategies seems to be a passable way forward. Instead, one might ask if there exists a "mixed strategy" that reaches a better social outcome than either of the pure options; and if so, what can be the role of privacy-enhancing technologies.

Nevertheless (even imperfect) privacy-enhancing technologies are relevant, though the focus on core technologies might differ somewhat.

5.2 User-controlled identity management systems for Privacy4Life

Looking at identity management (IdM) and in particular at user-controlled identity management systems, [HaPS08] have elaborated important requirements taking into account Privacy4Life. These requirements which address developers of IdM systems as well as application providers[21], are summarised in the following:

[21] Note that some of the requirements or criteria have been mentioned before in other settings when discussing identity management in general. This section focuses on user-controlled identity management systems and primarily addresses developers and providers of IdM systems.

IdM-Req: Developers of IdM systems and application providers should provide mechanisms to represent data such as attributes and attribute values in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should provide mechanisms to establish, evolve, and use partial identities from personal data such as attributes and attribute values.

IdM-Req: Developers of IdM systems and application providers should support third-party certification of attribute values of partial identities in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should support (privacy-enhancing) reputation systems in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should support authentication of actions w.r.t. partial identities.

IdM-Req: Developers of IdM systems and application providers should support the user in deciding which attributes and attribute values are revealed to whom.

IdM-Req: Developers of IdM systems and application providers should support users to store and make easily accessible the history which attributes and attribute values have been communicated to whom in which context.

IdM-Req: Developers of IdM systems and application providers should support delegation concerning all or specifically selected actions, contexts, and/or partial identities.

IdM-Req: Developers of IdM systems and application providers should support migration to other technologies, i.e., migration to other user devices and other communication infrastructure as well as use for new applications.

IdM-Req: Developers of IdM systems and application providers should maintain usability so that users can avoid errors as well as perceive their own digital life as continuous.

These requirements which are in line with the requirements in the chapters before, but are limited to user-controlled identity management systems only, name already a few technological concepts. Many of these concepts are already part of the PRIME's blueprint of a user-controlled identity

management system [LeSH07][22], some have been added to reflect interactions among peers (for example, the reputation system), long-term aspects (for example, the necessity to make migration possible and refrain from lock-in effects), or stages of life (for example, the support of delegation).

The following section deals with technical primitives which are basic building blocks for user-controlled identity management systems.

5.3 Important technical primitives[23] and tools

We differentiate technical primitives and tools according to the following criteria:

1. The parties involved: Who is involved and what are their functionalities/abilities?
2. The purpose: What requirements does the primitive achieve for what information?
3. The attacker model: Against whom should the information be protected and who needs to be trusted?
4. The long-term problems: Which problems arise when the system is in use for a lifetime of an individual or even beyond?

It is especially important to not only consider these technical primitives and tools as technologies which already solve many challenges concerning Privacy4Life, but to apply the long-term perspective to them as well, in particular to show potential risks and conditions for their usage. This leads to further requirements when employing these technical primitives and tools which we point out in the following section.

5.3.1 Encryption schemes

Encryption schemes protect the confidentiality of the content of a text (but they do not protect communication-conjunctures if this text is sent, for instance who sends it from, where, when, to whom). There are two types of encryption schemes, the symmetric and the asymmetric scheme. Both types have three phases (key generation and possibly distribution, encryption, decryption): One symmetric secret key for encryption is created and distributed at least to the encryptor and to a possible decryptor in the first phase of symmetric encryption schemes. In the second phase, she encrypts the content to protect with this key. And in the third phase the decryptor (who might be the same person as the encryptor) decrypts the encrypted content. In asymmetric encryption schemes in the first phase a pair of public and private key is created by the decryptor who distributes the public key to possible encryptors who want to send messages to her. In the second phase, an encryptor encrypts the content to protect with this public key. Finally, the decryptor who holds the private key decrypts the encrypted content in the third phase.

1. The parties involved: There are an encryptor and possible decryptors of the message.
2. The purpose: Thereby both types of encryption schemes reach the following two properties:

---

[22] The FP6 project “PRIME – Privacy and Identity Management for Europe” is the predecessor project of PrimeLife. See also http://www.prime-project.eu/.

[23] The descriptions of primitives and tools are partly based on descriptions we already elaborated for the FP6 Network of Excellence “FIDIS – Future of Identity in the Information Society” (http://www.fidis.net/).
Please note we do not intend to write lecture notes on cryptography here so the summaries are pretty short just to introduce the schemes that are used later on for the tools. Detailed information of these concepts can be found in numerous books about cryptography.

- Confidentiality of the content.

3. The attacker model:
   - No attacker can break the confidentiality of the content (as long as the encryption scheme is not broken).
4. The long-term problems: If cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time.

There exist numerous implementations for encryption schemes; the most widely known symmetric one might be the onetime-pad and the most popular asymetric one RSA [RiSA78].

5.3.2 Secret sharing

(k,n)-Secret sharing was invented independently in [Sham79] and [Blak79] and means protocols for splitting secrets into *n* parts, called shares, which are distributed amongst a set of several participants. The secret can only be reconstructed when a subset *A* of the participants with *k* (with $k \leq n$) of the shares combine their shares; individual shares do not reveal any information on the secret. Generalised Secret Sharing as proposed in [BeLe88] overcomes the limit of (*k* out of *n*) but allows generic monotonic access structures to a secret. Monotonic here means that whenever a set *A* is sufficient to reconstruct a secret that also a set *A'* containing all members of *A* can reconstruct the secret.

1. The parties involved:
   - a so-called dealer, i.e., the initial owner of the secret[24],
   - shareholders, i.e., the participants who get shares, and
   - a reconstructor, i.e., the party that reconstructs the secret.
2. The purpose: For the secret that has to be protected secret sharing reaches a balance between the following two properties:
   - Availability: even if some shares are lost, the secret is not.
   - Confidentiality: an adversary who gains access to only a few shares has no advantage in guessing the secret.
3. The attacker model:
   - Regarding availability reconstruction works correctly, if dealer, reconstructor and the necessary shareholders participating in the reconstruction are honest and the communication between them is integer.
   - Regarding confidentiality any subset of shareholders not containing all of the ones in *A* gain no information about the secret as long as the dealer and the reconstructor are honest and the communication between them is confidential.
4. The long-term problems: Availablity of the share holders might decrease if no recursive structure is applied. In the case of a recursive structure the (non-existing) relation between the original owner of the secret and the share holders in a recursive structure might be critical for confidentiality and availabity.

---

[24] In general, the secret can also be generated in a distributed way so that no single entity ever knows the secret.

5.3.3 Attribute-based encryption

In an attribute-based encryption system as introduced by Sahai and Waters [SaWa05], a user's private keys and encrypted contents are labeled with sets of descriptive attributes. Every particular private key can decrypt a particular encrypted content only if there is a match between the attributes of the encrypted content and the user's private key.

1. The parties involved: An encryptor and possible decryptors of the content.
2. The purpose: Attribute-based encryption schemes reach confidentiality of a content against everyone who does not fulfil the attributes the content is labelled with.
3. The attacker model: No attacker can break the confidentiality of the content (as long as the encryption scheme is not broken).
4. The long-term problems: If cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time.

5.3.4 Commitments

A commitment scheme allows one party to commit to a secret (fix it so that it cannot be changed) without telling another party about it for a certain time. After telling the other party the secret this party is able to verify that this was the secret the first one committed to. Commitments were first invented as unnamed primitives in other protocols, for example, zero-knowledge proof systems, and only later recognised as something that deserves a name because it occurs so often. The first systematic treatment can be found in [BrCC88].

1. The parties involved: A so-called committer and a recipient of the committed secret.
2. The purpose: Commitment schemes have a first phase after which the committer is committed to a secret, but the recipient cannot see it yet, and a second phase for opening and verifying the commitment. Thereby it reaches the following two properties:
   - Committing property: The committer cannot change the secret after the first phase.
   - Confidentiality property: The recipient does not learn anything about the secret during the first phase.
3. The attacker model:
   - Regarding the committing property even a dishonest committer cannot open one commitment in two different ways.
   - Regarding the confidentiality property the first phase does not give the recipient any information about the secret.
4. The long-term problems: If cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time.

5.3.5 Zero-knowledge proofs

Zero-knowledge proofs were first presented in 1985 by Shafi Goldwasser, et al. [GoMR85]. With a zero-knowledge proof one party is able to prove to another party that a statement she made is true, without revealing anything other than the truth of the statement.

1. The parties involved: A so-called prover of the statement made and a verifier of the proof.

2. The purpose: A zero-knowledge proof should fulfil the following properties:
   - Completeness: The prover can convince the verifier of correct statements.
   - Soundness: Not even a dishonest prover can convince an honest verifier of wrong statements.
   - Zero-knowledge: None who interacts with the prover gets any new knowledge about her statement except she explicitly reveals information on it.
3. The attacker model:
   - If the prover is dishonest and her statement is false she cannot convince the honest verifier that it is true.
   - Even if the verifier is dishonest he cannot learn anything other than the truth of the statement proved by the zero-knowledge proof.
4. The long-term problems: If cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time.

5.3.6 Blind signatures

Blind signatures allow one party (recipient) to have a message signed by a second party (signer), whereas the second party is neither able to link the signature with the protocol session during which the signature is created nor with the identity of the original party holding the message and the corresponding signature.

1. The parties involved: A signer and a recipient and possible verifiers of the signature.
2. The purpose: In contrast to traditional signature schemes blind signature schemes have five instead of three phases: In the first phase (the key generation and distribution) the signer creates public and private key for a digital signature scheme and distributes the public key. In the second phase (the blinding) in contrast to traditional signature schemes the text to be signed, is generated by the recipient of the signature (not by the signer) who blinds it (usually by encryption) and sends it to the signer. . In the third phase the signer validates that the received input corresponds to the expected content. Even thought the signer is not able to read the content from the blinded input directly, he can verify that the content matches the expectation by utilizing “cut-and-choose” or “zero-knowledge” protocols. In the fourth phase (the signing) the signer signs the blinded text and sends it to the recipient. In the fifth phase (the un-blinding) only the recipient knows how to un-blind the original text and is able to transform the signature to the blinded text to a signature to the un-blinded text. In the sixth phase (the verification) everyone who knows the signer’s public key can verify if the signature fits to the text. Thereby blind signatures reach the following two properties:
   - Unlinkability of blinded and un-blinded text as well as unlinkability of the signatures to them.
   - Integrity of blinded text and un-blinded text by the signatures on them.
3. The attacker model:
   - None except the recipient knows the linkability of text and blinded text resp. blinded signature and signature.
   - No attacker can break the integrity of the text resp. blinded text as long as the signature scheme is not broken.

4. The long-term problems: As cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time. The necessary public-key infrastructure has to be sustained for a long time.

5.3.7 Pseudonymous convertible credentials

A credential system is a system in which data subjects can obtain credentials from organisations and demonstrate possession of these credentials. Credentials usually are assigned to pseudonyms. With convertible credentials the data subjects are able to transform a credential issued to one of her pseudonyms to another one of her pseudonyms. This concept was introduced in [Chau86].

1. The parties involved: Users and organisations.
2. The purpose: In an anonymous credential system organisations know the users only by pseudonyms. An organisation can issue a credential to a pseudonym, whose holder can convert this credential to another pseudonym of hers. Then she can prove possession of this converted credential to another organisation and the following properties hold:
   - Integrity of the converted credential.
   - Unlinkability of credential and converted credential and thereby unlinkability of the pseudonyms they are used with.
3. The attacker model:
   - Regarding integrity it should be impossible for a user and other organisations to forge a credential of another organisation for the user, even with an adaptive attack on the respective organisation.
   - Regarding unlinkability an organisation cannot find out if two pseudonyms belong to the same user as far as the user does not tell it.
4. The long-term problems: As cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time. The necessary public-key infrastructure has to be sustained for a long time.

In [CaLy01] such a credential system is called anonymous. This term might be misleading because the system does not reach anonymity directly, but only pseudonymity by the use of pseudonyms and unlinkability. This might result in anonymity, but does not necessarily do so if person pseudonyms are used.

5.3.8 Pseudonyms

Pseudonyms act as identifiers of subjects or sets of subjects. Whereas anonymity on the one hand and unambiguous identifiability on the other are extreme cases with respect to linkability to subjects, pseudonymity comprises the entire field between and including these extremes [PfHa08].

1. The parties involved: The holder of the pseudonym and the parties she uses her pseudonym with.
2. The purpose: Important properties of pseudonyms can include [ClKo01]:
   - Proof of holdership: Digital pseudonyms could be realised as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature which is created using the corresponding private key.
   - Linkability due to the use of a pseudonym in different contexts

- Convertability, i.e., transferability of attributes of one pseudonym to another: The user can obtain a convertible credential (see above) from one organisation using one of her pseudonyms, but can demonstrate possession of the credential to another organisation without revealing her first pseudonym.
- Authorisations can be realised by credentials or attribute certificates bound to digital pseudonyms, but also in case of digital vouchers transferable to other people by blind signatures (see above) as well.

3. The attacker model:
   - The users can determine the linkability of her pseudonyms hersely.
   - Attacker model of convertible credentials applies to convertability.
   - No attacker can break the holdership of a pseudonym and the correctness of authorisations as long as the signature scheme used is not broken.
4. The long-term problems: Pseudonyms used for a long time allow long-term profiles.

5.3.9 Steganography

Steganography is the old art and the young science of hiding secret information in larger, harmless looking files, the so-called cover data. The main difference to cryptography is: If good cryptography is used, the attacker notices that she cannot understand the cryptotext and will hence presume that the communication is confidential. But if good steganography is used, the attacker will think that the cover data is a plausible message which he completely understood. She does not notice any confidential communication. The young science of steganography uses computers to embed secret data for example in digitalised pictures, video signals or sound signals. According to Kerkhoffs' principle, the security of steganographic systems must not depend on the secrecy of the steganographic algorithm but on a key used to parameterise the embedding. Symmetric keys distributed before exchanging secret messages can be used to control the embedding process itself. To increase security, cryptographic systems can be used to encrypt messages before embedding [ZFK+98].

1. The parties involved: A sender who embeds the secret message into the cover data, and a recipient who extracts the message.
2. The purpose: The purpose of steganographic systems is to hide not only the secret message, but also even its existence. This is helpful if confidential communication is suspicious, unwanted or even illegal.
3. The attacker model: An attacker must not be able to decide with probability better than random guessing whether suspected data contains steganographically embedded messages or not.
4. The long-term problems: If cryptographic assumptions are made, the key length has to be chosen carefully to provide protection for a long time. The attacker must not get a better model of the cover data as the sender.

5.3.10 Secure logging

Secure logging of a system's events is needed to find privacy evidences caused in the procession of personal data.

1. The parties involved: Data controller and possibly also the data subject.

2. The purpose: The data controller is interested in logging all actions which support the impression that she behaves according to the privacy policies, but he is definitely not interested in logging any action which could be taken as evidence for abusing the personal data of the data subject. The data subject is interested in accurate and complete logs, but particularly in those entries which could be an evidence for the abuse of her personal data.
3. The attacker model: Forward integrity for log entries assures that previous entries cannot be altered, even if the system is compromised. Additionally the deletion of log entries should corrupt all subsequent log entries to reach completeness of log data.
4. Long-term logs pose an increasing risk on the respective users' privacy.

[BeYe97] introduce the application of message authentication codes (MACs) in order to be reach forward integrity. They divide the timeline into several epochs and use different keys for the message authentication in each epoch with the authentication keys destroyed at the end of each epoch. The authentication key for each epoch is derived from the key of the previous epoch. The derivation of new keys has to be done by a non-reversible mapping such that the attacker is not able to reverse this step and obtain a key of a previous epoch. However an auditor is able to check the authenticity of all log entries by reproducing the MAC keys from the the first authentication key. This protocol makes changes in the log entries apparent to the auditor, but does not help out when the attacker deletes log entries within an epoch.

To reach completeness of log entries either sequence numbers as proposed by [BeYe97] or hash chains as proposed by [ScKe99] can help. In a hash chain for log entries, the hash of the current log entry does not only depend on the content of the log entry, but also on the hash of the previous log. Thus, the hash of a log entry would only be reproducible as long as the hash value of the previous log entry exists (and is valid).

The data controller has a clear advantage over the data subject by means of deciding on which actions to log. [AcBe07] suggest using trusted computing in order to assure that continuous and non-selective logging of all events is performed by the data processor. Once personal data have to leave the trusted environment, secure logging can only provide privacy evidences for the leakage, but not for any further processing.

In general, logs of data processing can be understood as metadata of the processed data. Thus, the less logs exists the less mechanisms are necessary to protect the (meta) data against unauthorised access (or leakage) and the easier it is to reason for privacy properties of a protocol or system. Logging and the need for audits is in fact, whenever involving personal data, causing new privacy issues that need to be addressed in a careful manner in order to let the protocol or system benefit and not suffer from the logging.

5.3.11 Linking the technical primitives to the requirements

The high-level requirements from Section 3.1 have not been designed to be implemented solely or predominantly by technological means. So it is no surprise that Table 1 shows that the technical primitives do not cover all areas the requirements address. Most of the primitives stem from the PET core theme of data minimisation. However, they do not stop when implementing data minimising functionality, but also address fair use issues and could be part of user-controlled identity management functionality. In addition, they may be employed in privacy-enhancing feedback mechanisms which support change management on a societal basis.

	Transparency	Data minimisation	Fair use	User-controlled IdM	Practicability of mechanisms	Change management
Encryption		x	x	x		
Secret sharing		x	x	x		
Attribute-based encryption		x	x	x		
Commitments		x	x	x		x
Zero-knowledge proofs		x	x	x		
Blind signatures		x	x	x		x
Credentials		x	x	x		x
Pseudonyms		x	x	x		x
Steganography		x		x		
Secure logging	x		x	x		

Table 1: Linking technical primitives to high-level requirements

Although the requirements for user-controlled identity management systems (cf. Section 5.2) address more directly technical concepts, the attempt to assign the primitives to those requirements reveals the different layers of the approaches. It is true that all technical primitives can play a role in user-controlled identity management systems, and this is easy to understand for basic and widely distributed modules such as encryption tools or for the core technologies for user-controlled identity management such as pseudonyms or pseudonymous convertible credentials. Also secure logging on trusted devices is clearly important for managing reliably one's partial identities. Other primitives help to implement specific functionality, such as secret sharing supports delegation or deciding on post-mortem or emergency access rights to one's partial identities. The following section discusses briefly additional requirements when combining technical primitives to tools or modules employed in user-controlled identity management systems.

5.4 Challenges when employing technical primitives for Privacy4Life

The analysis from the previous section shows that all mentioned technical primitives are vulnerable in the long term, and it is hard to imagine primitives in the realm of technology without that vulnerability. Technical progress over time (also including attack technologies) not only requires algorithms and architectures to be upgraded, but also impose a burden on current designs. While concepts as logging and digital signatures can be extended by binding them to the timeframe in which they were generated, communicated data can be recorded for future attacks such as advanced data mining or breaking of encryption algorithms. This means that any data, communicated over a network that allows for interception, can be exploited at a certain point in

time. For cryptographic techniques, the horizon of what we can predict is rather limited, because of possible theoretical breakthroughs. Experts are suggesting algorithm/key size combinations for long-term protection (approx 30 years); higher security levels are targeting "the foreseeable future" [Näs08]. It should also be noted that the (possible) development of sufficiently large quantum computers will reshape the entire cryptographic field. Another remark is that for signatures, a refresh mechanism can be used to "update" digital signatures (mostly done by time-stamping). Such a mechanism does not exist for encrypted data.

Robustness and resilience of cryptography is therefore discussed in the ICT security community [BuMV06]. It is not sufficient to choose a long key size for cryptographic algorithms if attackers may find other possibilities to break the codes. Moreover, if a cryptographic module which is part of a larger ICT system becomes insecure or vulnerable against attacks, this incident has to be dealt with. The design of the ICT system could integrate diverse cryptographic modules with different algorithms where it is unlikely that both fail at the same time. Then the system could switch to the other module. Of course this switch may also be a vulnerability of the ICT system – imagine an attacker switching the system to the weak protection level before attacking it. Currently there are very few products which contain already multiple diverse cryptographic modules to enhance its robustness.

In any case the technical primitives have to be built together and to be orchestrated by ICT systems such as a user-controlled identity management system. Not only cryptographic challenges will occur, but also possible interlinkages and dependencies between different primitives or tools may be problematic. Even updating certain modules may affect the interoperability of the components. Also migration to other systems should be supported which is not trivial either. In addition to the technical difficulties in the interplay of components the real-life settings may pose severe challenges, for example, if the user-controlled identity management system does not cover all potentially privacy-relevant areas of life and thereby cannot control the amount of data available to possible attackers who aim at identifying its pseudonymous user. Further the implemented algorithms run on today's (and future) hardware where it cannot be assumed that it fulfils the sufficient level of protection against attacks. Currently it is not probable that users will be equipped with trusted devices only they themselves can control – this may be not in the interest of States which have been discussing the necessity of backdoors for law enforcement or secret services for several decades.

5.5 Conclusion

PrimeLife's work on Privacy4Life so far has shown that there are no ready-made concepts that convincingly solve the challenges of maintaining privacy throughout one's life. In fact it seems to be a small area in academic discussions only. The purblindness of developers of ICT systems as well as application providers can be explained by the short- or medium-term requests on the market. In addition stability and security of today's technological solutions have to be improved for current purposes before long-term concepts will be tackled. Privacy-enhancing technologies and most of the sketched technical primitives can be rarely found in present ICT products. Thus, developers, providers, and users have to gain more experiences in the potential, usage, and also shortcomings of PETs. However, policy makers should be aware of the challenges of Privacy4Life and plan ahead.

Chapter 6

Recommendations for policy makers

Many of the above mentioned requirements in Chapters 3 and 4 do concern issues that are also relevant for policy makers. As stated in those previous chapters, existing regulations are often not sufficient to guarantee proper handling of personal data throughout life for the data subject. The law may be interpreted in different ways and in many situations there are no legal stipulations for the orientation in handling personal data.

Note that in our understanding the term "policy makers" comprises not only law makers setting legal standards, but also those entities that set standards by other means, in particular by standardisation of technology, but also by presenting best practices as guidelines for system developers or application providers. However, the issues pointed out in the following sections cannot be sufficiently handled only by technological solutions, so our recommendations should be reflected at least in the legal systems within Europe.

6.1 Openness, transparency, notice, awareness, understanding

To ensure transparency, policy makers need to clearly consider all consequences when deciding about new statutes regarding personal data. Especially revocation needs to be considered in each decision making process. Therefore policy makers have to take into account which situations may occur where revocation of personal data is necessary and which risks and effects new statues on personal data may have. One example may be identification numbers that are assigned to natural persons and where legislators have to clearly define on the revocability and to consider effects and risks of the ID number (for example, the taxID introduced in Germany in 2008 as unique identifier for each citizen where personal data may be accessible for unauthorised parties).

Transp-Req: Policy makers should define and explicate areas where revocable respectively irrevocable consequences are demanded respectively prohibited. This should guide system developers when conceptualising, designing and implementing ICT systems as well as application providers when operating applications.

In many situations throughout life the interpretation of law is various. Often definitions are unclear and leave room for all ways of interpretation or are not complete. Therefore, policy makers and supervisory authorities should make clear, what they demand from data controllers and data processors concerning privacy-relevant data processing, for example, how to interpret privacy regulations.

This problem, for example rises in the context of joint responsibilities for data processing. In many situations personal data may be relating to individuals but also to groups of individuals. Therefore the discussion raises how to handle personal data in case of joint responsibility of personal data. In general there is no "ownership" of data. Personal data relate to an identified or identifiable natural person, but is not a property. For this reason the wording "ownership" is not correct and a better way to name the situation would be joint responsibility. Every data subject is responsible for the data within his or her area of accountability. Therefore, for example it has to be asked for the consent if personal data of a third person should be processed (for example, posting of pictures in SNS).

Transp-Req: Policy makers and supervisory authorities should make clear what they demand from data controllers and data processors concerning privacy-relevant data processing, i.e., how to interpret privacy regulation.

6.2 Decreasing the risk to Privacy4Life by data minimisation

The concept of "pseudonymous convertible credentials" (cf. Section 5.3.7) provides privacy-enhancing ways to combine anonymity and accountability requirements in ICT systems: They enable a data subject to prove her authorisation whilst controlling the conditions determining her identifiability and accountability at the same time. However, to foster their employment in ICT systems, an appropriate infrastructure has to be built up, and the concept has to be reflected in legal provisions [LaRo08].

DatMin-Req: Policy makers should support setting up and standardising the necessary infrastructure for issuing pseudonymous convertible credentials and their usage in their ICT systems where appropriate.

DatMin-Req: Policy makers should evaluate current legal provisions in the light of pseudonymous convertible credentials.

6.3 Controllable and controlled data processing

This section lists a few recommendations concerning the legal provisions on data processing, the question of user control, sanctioning privacy infringements, conflicting policies, and delegation.

6.3.1 Real purpose binding

Considering long-term effects, some of the currently existing legal provisions could need some intensification. This applies to the principle of purpose binding which has been weakened by manifold exceptions as well as to handling of sensitive data:

Control-Req: Policy makers should further limit exemptions to use (potentially) personal data for other purposes.

Control-Req: Policy makers should be extra cautious with (potentially) sensitive data.

6.3.2 User control

The data subject is assumed to be an autonomous, privacy-aware individual, capable to act appropriately according to her own will. From the previous sections, it is clear that this ideal image is not true. This also affects principles such as “consent” which is a sufficient basis for data controllers to process personal data. But if the data subject cannot understand what she is consenting to, the consent is obviously not a useful solution. And in today’s complex world this may become the rule.

Control-Req: Policy makers should rethink the concept of consent and possibly limit data processing based on consent in its scope or extent.

Hence, the whole concept of user control has to be challenged: It should not be mistreated to shift the responsibility on to an overburdened individual, but users should be empowered so that they really can exercise their rights.

Control-Req: Policy makers should seek for ways to efficiently implement fair user control, easy to perform for all individuals.

6.3.3 Coping with privacy infringements

Most of the data protection laws already have regulations regarding sanctions for privacy infringements. Nevertheless they are often not applicable or enforceable and furthermore differentiate within the EU Member States. Therefore useful legal sanctions for responsible parties as well as remedies for victims should be legally stipulated.

Control-Req: Policy makers should revise the current framework for sanctioning privacy infringements and providing remedies for victims.

Control-Req: Supervisory authorities should sanction privacy infringements by noticeable punishments.

Control-Req: Policy makers should elaborate concepts for achieving remedy for victims of privacy infringements (“privacy infringement insurance”?).

6.3.4 Dealing with conflicting policies and multiple processors

When, for example, the data subject and the controller use different policies, the problem may appear that there are conflicts within the policies. There might be different preferences for data processing within the policies of the user and the controller. From the legal aspect, the data subject may define the policy for the handling of her personal data. If, for example, the controller wants to

use personal data for different purposes than defined in the data subject's policy, he does need the explicit consent of the data subject.[25] That means if a policy should be changed with regard to the purpose of the data processing, the consent is required.

From the technical point of view, it might be helpful to define structures for policies. Policies could have clearly defined contents that can not be changed by the parties involved. Other parts of the policy may be changed by the parties involved in a clearly defined way. One solution can be joint policy responsibility.

In general, policies can only be evolved for the future up to a certain level. But it also has to be possible to adjust policies to current technical and legal changes. Therefore mechanisms are needed that enhance and adjust policies to current changes.

This also raises the question what happens with the revised policy and if transitional periods have to be considered. To keep policies up to date there could be, for example, a yearly reminder for the data subject or the controller for the decision about a need of policy change. At the moment there are no processes and no transparency for the data subject.

Furthermore, there might appear a conflict if multiple processors are involved in data handling. Processors handle personal data on behalf of the controller and merely have an auxiliary function with regard to the processing.[26] With regard to Art. 17 of the Data Protection Directive, the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out. The carrying out of processing by a processor must be governed by a contract that stipulates that the processor shall act only on instructions from the controller.[27] Processors do not have to comply with the vast majority of requirements determined by the Data Protection Directive, but basically must follow the instructions of the controller and implement appropriate technical and organisational measures ensuring data security.

Control-Req: Policy makers should propose guidelines for how to deal with conflicting policies.

6.3.5 Delegation

As mentioned above[28] delegation may not only be useful for cases where the concerned individual is fully in possession of his/her mental capabilities and decides on her own to transfer the exertion of rights to another person. Proxies often are overtrained with their duties or even do not know the limitations of their responsibilities. Therefore law makers should define general principles or guidelines for handling of privacy by a proxy as an orientation.

Delegate-Req: For legally relevant settings, policy makers should regulate the circumstances of expressing and revoking delegation.

Delegate-Req: Policy makers should define general principles or guidelines for the handling of privacy by a proxy as an orientation.

---

[25] See above, Section 3.1.3.1.

[26] Art. 2 (g) of the Directive 95/46/EC

[27] The European Committee for Standardisation (CEN) has published an Article 17 Model Contract (Standard form contract to assist compliance with obligations imposed by Art. 17 of the Directive). This contract is online available at: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15292-00-2005-May.pdf.

[28] See above, Section 4.4.2.

Delegate-Req: Policy makers should provide rerequisites to enable later revision of privacy-relevant actions performed by the proxy on behalf of a data subject.

Delegate-Req: Policy makers should provide reasonable legal solutions to protect the proxy and to balance the interests of the proxy and the principal in a fair way.

6.4 Change Management

In Section 3.1, the necessity of dealing with changes has already been elaborated – primarily from the perspective of a data controller, but also other stakeholders have been mentioned:

ChangeMng-Req: Data controllers, data processors, system developers, and policy makers should monitor changes in society, law and technologies and react appropriately (for example, by evaluating chances and risks, adapting current processes, regulation or standards to the changed conditions etc.).

6.4.1 Ensuring legal compliance over time

Not only data controllers, but also supervisory authorities dealing with privacy and data protection have to tackle changes in law, in the state-of-the-art of technology. This has to be reflected in their regular work, e.g, when controlling legal compliance of data processing by disposing audits or seals of approval.

6.4.2 Reacting to societal changes – legal and technical aspects

It also has to be taken into account, that with a changing society also legal and technical aspects may change. Here the question raises how jurisdiction and technology react on these changes and how in general these changes can be recognised. This could be on the one hand by the feedback of the society and it can be used to try to develop law and technologies compliant to the changes. Therefore changes have to be achieved by developers. Developers need feedback mechanisms to react on society changes with legal and technical implementations. To enable evaluation and feedback building safeguarding technologies may (deliberately) reduce degrees of freedom in action and freeze the current state of policy. However, technology should not work against evolvement of societal consensus. Thus, solutions should take into account the possibility to evaluate whether the current state is still considered alright and provide for an optional feedback if changes are desired. For this feedback it is also important to consider privacy implications, for example, providing possibilities for individuals giving feedback to stay anonymous [Phil04].

ChangeMng-Req: Policy makers should establish (privacy-enhancing) feedback mechanisms for society concerning privacy-relevant changes (for example, on attitudes what is to be considered private or public).

ChangeMng-Req: Policy makers should establish (privacy-enhancing) feedback mechanisms for society concerning privacy-relevant regulation, processes and technical implementations.

6.4.3 Ex ante privacy assessment of technical advancement and legislation of emerging technologies

Today, development of privacy law is mostly one step behind technological developments. Amendment of law only responds to insights into the consequences of advances in the processing and analysis of personal data [Kirb08]. Preventive approaches on revising privacy law in the light of expected advances in technology are not common, and developing high-level concepts or formal models for a systematic assessment of emerging technologies is still work in progress [CHP+09]. Dommering even emphasises: "When a technology reaches a vast diffusion it affects society in a way which was not part of the design" [Domm06].

Prior checking and technology assessment are two instruments which should enable more than a glimpse on what implications upcoming technologies or ICT systems may have concerning privacy. This should also be intensified in the law-making process. In particular the assessment should be done in an interdisciplinary approach comprising lawyers, technologist, sociologists, psychologists, economists, perhaps also philosophers, historians, or physicians. This enables a broader discussion on potential cross-effects and should yield a wider perspective on the possible implications.

ChangeMng-Req: Policy makers should demand and support ex ante privacy assessments of technical, regulatory, and legislatory advancements.

This also applies to standardisation activities or funding of projects.

ChangeMng-Req: Policy makers should consider the state-of-the-art and research results concerning privacy-enhancing technologies as well as potentially privacy-infringing technologies in law making, standardisation, funding and other supporting actions.

6.5 Conclusion

This chapter shows that especially for policy makers it is quite a challanging task to enable identity management throughout life. This Heartbeat is not exhaustive and only addresses main problems in selected scenarios. But in general, policy makers need to adjust privacy policies to current social and technical development.

Chapter 7

Conclusion and outlook

This Heartbeat provides an analysis of requirements and concepts for identity management throughout life. It is shown, that there are still legal and technical gaps with respect to identity managmement in daily life throughout one's whole life. Therefore possible requirements and recommendations on selected scenarios were derived within this deliverable to help various stakeholders like policy makers, developers and providers of applications and ICT infrastructures, third parties which can support Privacy4Life, and users or other data subjects to handle daily life identity management.

However, this is only shown on selected scenarios within this Heartbeat and the selection of scenarios is not exhaustive. Within this text we have emphasised some fundamental issues for privacy management throughout life and defined several requirements and concepts calling for further refinement and attention by legal and technical entities. The definition of requirements and concepts is calling for further refinement and attention by future research. In conclusion this Heartbeat shows that in the context of privacy and identity management throughout life specific issues arise that cannot be solved very easily. Especially the combination of technical and legal aspects is challenging to solve.

References

[AcBe07] R. Accorsi and M. Bernauer. On privacy evidence for UbiComp environments – Broadening the notion of control to improve user acceptance. In: A. Bajart, H. Müller, and T. Strang (eds.): *Proceedings of the 5th Workshop on Privacy in UbiComp,* pp. 443-438. 2007.

[AcGr05] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26-33, 2005.

[Arti03] Article 29 Data Protection Working Party. *Working Document on biometrics of 1 August 2003.* 12168/02/EN, Working Paper 80. Brussels, Belgium, 2003. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf (current Nov. 2009).

[Arti05] Article 29 Data Protection Working Party. *Working Document on a common interpretation of Article 26(1) of the Directive 95/46/EC of 24 October 1995.* 2093/05/EN, Working Paper 114. Brussels, Belgium, 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf (current Nov. 2009).

[Arti07] Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data.* 01248/07/EN, Working Paper 136. Brussels, Belgium, 2007. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf (current Nov. 2009).

[Arti09a] Article 29 Data Protection Working Party. *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).* Working Paper 160, 398/09/EN, adopted on 11 February, 2009. Brussels, Belgium. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf (current Nov. 2009).

[Arti09b] Article 29 Data Protection Working Party. *Opinion 5/2009 on online social networking*. Working Paper 163, 01189/09/EN, adopted on 12 June, 2009. Brussels, Belgium. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (current Nov. 2009).

[Bara65] P. Baran. *Communications, computers and people.* Technical report, RAND Corporation, Santa Monica, CA, 1965.

[BeLe88] J. Benaloh and J. Leichter. Generalized Secret Sharing and Monotone Functions. In: S. Goldwasser (ed.): *Advances in Cryptology*, Proceedings of CRYPTO '88, LNCS Vol. 403, pp. 27-35, Springer-Verlag, New York 1990.

[BeYe97] M. Bellare and B. Yee. *Forward integrity for secure audit logs.* Technical report, University of California at San Diego, Dept. of Computer Science & Engineering, 1997.

[Blak79] G. R. Blakley. Safeguarding cryptographic keys. In: *Proceedings of the National Computer Conference*, Vol. 48, pp. 313-317, AFIPS Press, New York, NY, USA, June 1979.

[Boyd08] D. M. Boyd. *Taken out of context. American Teen Sociality in Networked Publics*. PhD thesis, University of California, Berkeley, CA, USA, 2008. http://www.danah.org/papers/TakenOutOfContext.pdf (current Nov. 2009).

[BrCC88] G. Brassard, D. Chaum, and C. Crepeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156-189, 1988.

[BuMV06] J. Buchmann, A. May, and U. Vollmer. Perspectives for cryptographic long-term security. *Communications of the ACM,* Vol. 49, No. 9, pp. 50-55, 2006.

[CaLy01] J. Camenisch and A. Lysyanskaya. An efficient system for nontransferable anonymous credentials with optional anonymity revocation. In: *EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques,* LNCS Vol. 2045, pp. 93-118, London, UK, 2001. Springer-Verlag.

[Came05] K. Cameron. *The Laws of Identity*. Kim Cameron's Identity Weblog at http://www.identity.blog.com/, May 2005. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (current Nov. 2009).

[Came06] Kim Cameron. *Kim Cameron's Identity Weblog: Laws of identity in brief.* Website, 8 January, 2006. URL http://www.identityblog.com/?p=354 (current Nov. 2009).

[Chau81] D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM,* Vol. 24, No. 2, pp. 84-88, 1981

[Chau85] D. Chaum. Security Without Identification: Card computers to Make Big Brother Obsolete. *Communications of the ACM,* Vol. 28, No. 10, pp. 1030-1044, 1985.

[Chau92] D. Chaum. Achieving electronic privacy. *Scientific American,* pp. 96-101, August 1992.

[CHP+09] S. Clauß, M. Hansen, A. Pfitzmann, M. Raguse, and S. Steinbrecher. Tackling the challenge of lifelong privacy. In: P. Cunningham and M. Cunningham (eds.): *Proceedings of eChallenges 2009,* 2009.

[CLG+08] S. M. Cohen, M. de Lussanet, A. Garon, and D. Wilkos. *Multiple identities allow teens to create boundaries in online social networks. Email, IM, and social network strategists: Help teens manage multiple IDs while preserving privacy.* Technical report, Forrester Research, 9 September, 2008. http://www.forrester.com/go?docid=47006 (current Nov. 2009).

[ClKo01] S. Clauß and M. Köhntopp. Identity Managements and Its Support of Multilateral Security. *Computer Networks,* Vol. 37, No. 2, pp. 205-219, 2001.

[Comm07] Commission of the European Communities. *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*. COM(2007) 228 final, Version May 2, 2007. http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf (current Nov. 2009).

[Cris98] B. Crispo. Delegation of Responsibilities. In: B. Christianson et al. (eds.): *Security Protocols,* LNCS Vol. 1550, pp. 118-124, Springer, Berlin, Heidelberg, Germany 1998.

[Domm06] E. J. Dommering. Regulating technology: code is not law. In: E. J. Dommering and L. F. Asscher (Eds.), *Coding Regulation: Essays on the Normative Role of*

Information Technology, The Hague, The Netherlands, pp. 1-17, 2006. http://www.ivir.nl/publications/dommering/Regulating_technology.pdf (current Nov. 2009).

[ECHR50] *Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11.* Rome, 4 November, 1950, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (current Nov. 2009).

[Euro95] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal of the European Communities of 23 November 1995, No L 281, pp. 31-39.

[Euro02] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* Official Journal of the European Communities of 31 July 2002, No L 201, pp. 37-47.

[FCA+06] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick, and A. Costa-Pereira. How to break access control in a controlled manner. In *19th IEEE International Symposium on Computer-Based Medical Systems (CBMS 2006)*, pp. 847-854, 2006.

[FiWZ09] S. Fischer-Hübner, E. Wästlund, and H. Zwingelberg (eds.). *UI prototypes: Policy administration and presentation version 1.* Deliverable D4.3.1 of the EC FP7 project PrimeLife, 2009. http://www.primelife.eu/ (current Nov. 2009).

[Goff59] E. Goffmann. *The Presentation of Self in Everyday Life.* Doubleday Anchor Books, Garden City, New York. 1959.

[GoMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In: *STOC '85: Proceedings of the seventeenth annual ACM symposium on Theory of computing,* pp. 291-304, ACM Press, New York, NY, USA, 1985.

[GoWB97] I. Goldberg, D. Wagner, and E. Brewer. Privacy-enhancing technologies for the Internet. In: *Proc. of 42nd IEEE Spring COMPCON*, pp. 103-109, 1997.

[HaMe07] M. Hansen, S. Meissner (eds.). *Verkettung digitaler Identitäten.* (Engl.: *Linkage of digital identities.*) Report commissioned by the German Ministry of Education and Research, Kiel/Dresden, Germany, 2007. https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf (current Nov. 2009).

[HaPS08] M. Hansen, A. Pfitzmann, and S. Steinbrecher. Identity Management throughout one's whole life. *Information Security Technical Report (ISTR)*, pp. 83-94, 2008.

[Kirb08] M. Kirby. *Law making meets technology.* In: ON LINE opinion, 2008. http://www.onlineopinion.com.au/view.asp?article=7082&page=0 (current Nov. 2009).

[Korf09] D. Korff. Are Users of Social Networking Sites Subject to Data Protection Law, As Controller? In: *Data Protection Review* No. 9, June 2009. http://www.dataprotectionreview.eu/ (current Nov. 2009).

[Kune07] C. Kuner. *European data protection law: corporate compliance and regulation.* 2nd ed., 2007.

[LaRo08] M. Langheinrich, M. Roussopoulos (eds.). *Technology-Induced Challenges in Privacy & Data Protection in Europe – A Report by the ENISA Ad Hoc Working Group on Privacy & Technology.* Heraklion, Greece, 2008. http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe (current Nov. 2009).

[LeSH07] R. Leenes, J. Schallaböck, and M. Hansen (eds.). *PRIME White Paper.* 2007. https://www.prime-project.eu/prime_products/whitepaper/ (current Nov. 2009).

[Maye07] V. Mayer-Schönberger. *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing.* John F. Kennedy School of Government – Harvard University, Faculty Research Working Papers Series no. RWP07-022, April 2007. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976541 (current Nov. 2009).

[Mein09] M. Meints. The Relationship between Data Protection Legislation and Information Security Related Standards. In: V. Matyáš, S. Fischer Hübner, D. Cvrcek, and P. Švenda (eds.): *The Future of Identity in the Information Society.* 4th IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School, Brno, Czech Republic, September 1-7, 2008, Revised Selected Papers, pp. 254-267.

[Näsl08] M. Näslund (ed.): *ECRYPT Yearly Report on Algorithms and Keysizes (2007-2008), Chapter 7: Recommended Key Sizes.* http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.28-1.1.pdf (current Nov. 2009).

[OECD80] Organisation for Economic Co-operation and Development (OECD). *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.* 23 September, 1980. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (current Nov. 2009).

[Parna94] D. L. Parnas. Software aging. In: *ICSE '94: Proceedings of the 16th international conference on Software engineering*, pp. 279-287, IEEE Computer Society Press, Los Alamitos, CA, USA, 1994.

[PfHa08] A. Pfitzmann and M. Hansen. *Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology.* Working Paper v0.31. February 2008. http://dud.inf.tu-dresden.de/Anon Terminology.shtml (current Nov. 2009).

[Phil04] D. J. Phillips. Privacy policy and PETs – the influence of policy regimes on the development and social implications of privacy enhancing technologies. *New Media & Society,* Vol. 6, No. 6, 691-706, SAGE Publications, London, Thousand Oaks, CA and New Delhi, 2004.

[Pove99] D. Povey. Optimistic security: A new access control paradigm. *Proceedings of the 1999 workshop on New security paradigms,* pp. 40-45, New York, NY, USA, ACM, 1999.

[PRCD09] Q. Pham, J. Reid, A. McCullagh, and E. Dawson. On a Taxonomy of Delegation. In: D. Gritzalis and J. Lopez, (eds.): *SEC 2009*, IFIP AICT 297, pp. 353-363, IFIP International Federation for Information Processing, Springer, Boston, USA, 2009.

[PSCP08] R. Peeters, K. Simoens, D. De Cock, and B. Preneel. Cross-Context Delegation through Identity Federation. In: A. Brömme, C. Busch and D. Hühnlein (eds.):

BIOSIG 2008, LNI vol. 137, pp. 79-92, GI, Köllen Verlag, Bonn, Germany, 2008.

[RiSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 21:120–126, 1978.

[SaWa05] A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In: *Advances in Cryptology, Eurocrypt,* LNCS Vol. 3494, pp. 457-473, Springer, 2005.

[ScKe99] B. Schneier and J. Kelsey. Secure Audit Logs to Support Computer Forensics. *ACM Transactions on Information and System Security (TISSEC),* Vol. 2, Issue 2, pp. 159-176, 1999.

[SeAn08] W. Seltzer and M. Anderson. Using Population Data Systems to Target Vulnerable Population Subgroups and Individuals: Issues and Incidents. In: J. Asher, D. Banks, and F.J. Scheuren (eds.): *Statistical Methods for Human Rights,* Springer, pp. 273-328, 2008.

[Sham79] A. Shamir. How to share a secret. *Communications of the ACM,* Vol. 22, No. 11, 612-613, 1979.

[Simi06] S. Simitis. *Bundesdatenschutzgesetz.* 6. Auflage, 2006.

[ZFK+88] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modeling the security of steganographic systems. In: *Information Hiding,* pp. 344-354, 1998.

List of Abbreviations

Art.	Article
COPPA	Children's Online Privacy Protection Act
EC	European Commission
ECHR	European Convention on Human Rights
eID	Electronic ID (usually a credential to prove one's identity)
EU	European Union
FIDIS	Future of Identity in the Information Society (FP6 Network of Excellence)
ICT	Information and Communication Technologies
ID	Identifier
IdM	Identity Management
IFIP	International Federation for Information Processing
OECD	Organisation for Economic Co-operation and Development
PETs	Privacy-Enhancing Technologies
PRIME	Privacy and Identity Management for Europe (FP6 project)
Privacy4Life	"Privacy for life" (concept which is elaborated in PrimeLife's Work Package 1.3)
SNS	Social Networking Service
TURBINE	TrUsted Revocable Biometric IdeNtitiEs (FP7 project)
UI	User Interface
UK	United Kingdom
US	United States
USA	United States of America

List of Requirements

Transp-Req: For all parties involved in privacy-relevant data processing, it is necessary that they have clarity on the legal, technical, and organisational conditions setting the scope for this processing (for example, clarity on regulation such as laws, contracts, or privacy policies, on used technologies, on organisational processes and responsibilities, on data flow, data location, ways of transmission, further data recipients, and on potential risks to privacy).

DatMin-Req: Data minimisation means to minimise risks to the misuse of these data. If possible, data controllers, data processors, and system developers should totally avoid or minimise as far as possible the use of (potentially) personal data, conceivably by employing methods for keeping persons anonymous, for rendering persons anonymous ("anonymisation"), or for aliasing ("pseudonymisation"). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible. Policy makers should implement the data minimisation principle in their work, be it in law making or technological standardisation.

Control-Req: For all parties involved in privacy-relevant data processing, the processing should be controllable and controlled throughout the full lifecycle. It should be compliant with the relevant legal and social norms.

ChangeMng-Req: Data controllers, data processors, and system developers should monitor changes in society, law and technologies and react appropriately (for example, by evaluating chances and risks, adapting current processes, regulation or standards to the changed conditions etc.).

Transp-Req: Schools or education centres should make individuals aware of potential risks to privacy and ways to deal with these risks.

Transp-Req: Data controllers and data processors should make their employees aware of potential risks to privacy concerning data processing and ways to deal with these risks.

Transp-Req: Parents should make their children aware of potential risks to privacy and ways to deal with these risks.

Transp-Req: For all parties involved in privacy-relevant data processing, it should be clear under which circumstances decisions are revocable/irrevocable and what the potential impact can be. In particular, data controllers should inform data subjects on to which degree their decisions (such as consent to processing of personal data or distribution of these data) are revocable or not.

Transp-Req: Data controllers and data processors should keep audit trails on the privacy-relevant data processing.

Transp-Req: For audit trails, data controllers and data processors have to define and make transparent (at least within the organisation and for supervisory authorities) which information is logged for how long.

Transp-Req: For audit trails, data controllers and data processors have to define and make transparent (at least within the organisation and for supervisory authorities) who can get access to the log data under which conditions.

Transp-Req: Data controllers and data processors should inform data subjects about the logic behind data processing (for example, in profiling systems) in a comprehensible way.

Transp-Req: In case other regulation inhibits detailed information for data subjects, data controllers and data processors should make the logic behind data processing transparent for supervisory authorities.

Transp-Req: Data controllers and data processors should make transparent for data subjects, under which conditions (potentially) personal data may be, will be or actually are linked.

Transp-Req: Data controllers and data processors should inform data subjects concerned and supervisory authorities timely on privacy and security breaches and give advice on how to cope with the (potential) consequences.

DatMin-Req: Data controllers and data processors, and system developers should minimise the storage of (potentially) personal and sensitive data as far as possible.

DatMin-Req: Supervisory authorities and privacy organisations should support individuals, data controllers and data processors, and system developers to fulfil the principle of data minimisation by giving advice concerning concepts and implementations, pointing to best practices and support research and development in this field. This may be done by employing methods for keeping persons anonymous, for rendering persons anonymous (“anonymisation”), or for aliasing (“pseudonymisation”). Observability of persons and their actions as well as linkability of data to a person should be prevented as far as possible. If (potentially) personal data cannot be avoided, they should be erased as early as possible.

DatMin-Req: Data controllers and data processors, and system developers should minimise the timeframe of storage and use of (potentially) personal data as far as possible. After that time, the data should be fully erased. This should comprise temporary files or data which have been distributed to other media or recipients as far as possible.

DatMin-Req: Data controllers, data processors as well as individuals should minimise the disclosure of (potentially) personal data as far as possible.

DatMin-Req: Data controllers and data processors, and system developers should minimise linkability and linkage of (potentially) personal data as far as possible.

DatMin-Req: Data controllers and data processors, and system developers should minimise multi-purpose or context-spanning use of (potentially) personal data as far as possible. They should provide mechanisms for context separation of these data.

DatMin-Req: Data controllers and data processors, and system developers should avoid the use of unique identifiers which may be used in different contexts. They should use diverse identifiers where possible.

DatMin-Req: Data controllers and data processors, and system developers should support anonymous or pseudonymous authorisation and access control of users where possible.

DatMin-Req: Data controllers and data processors, and system developers should minimise irrevocable consequences concerning the privacy of data subjects.

DatMin-Req: For societally relevant services which may be accessed in an anonymous or pseudonymous way, data controllers and data processors should not make the rendering of services contingent upon the consent of the user to the processing or use of her data for other purposes if other access to these services is, not or not reasonably, provided to the user.

Control-Req: Data controllers and data processors should restrict the processing of (potentially) personal data to a predefined purpose.

Control-Req: Data controllers and data processors should be specific in the definition of the respective purposes.

Control-Req: If the data processing is based on consent: Data controllers should limit the data subject's consent in time by default.

Control-Req: If the data processing is based on consent: Data controllers should ensure that the data subject can withdraw the consent without unexpected impacts on his privacy (because of irrevocable consequences).

Control-Req: Data controllers and data processors should ensure that the parties processing the data are accountable. This includes the definition and assignment of clear responsibilities.

Control-Req: Data controllers and data processors should prohibit identity theft, especially in situations which may have privacy-infringing impacts

Control-Req: Data controllers and data processors should conceptualise and plan their privacy-relevant data processing beforehand, thereby covering the full lifecycle of data (from creation to deletion). This comprises to plan the process and set the conditions for potential or factual linkage of data and – if the data processing is based on consent – also for its revocation.

Control-Req: If identifiers are created, data controllers and data processors should already foresee concepts and procedures for their erasure after the usage period.

Control-Req: Data controllers and data processors should also plan for emergency situations (for example, privacy and security breaches).

Control-Req: Data controllers should prevent lock-in situations. For example, SNS providers should provide portability for user profiles.

Contrtol-Req: Data controllers, and in SNS also peers, should clearly define responsibilities in case of joint responsibility of data as well as the rules for jointly or separately using the joint data (for example, in a (privacy) policy or another binding contract).

Control-Req: Data controllers and data processors should be extra cautious with (potentially) sensitive data.

Control-Req: Data controllers should provide the appropriate information to the data subject to create transparency of what kind of privacy-relevant data is processed by whom. Further they should support data subjects in exercising their rights, e.g., by lowering the threshold to get access to personal data via online solutions.

Delegate-Req: Data controllers, data processors, and system developers should foresee that data subjects can delegate their identity management to proxies.

Delegate-Req: Data controllers, data processors, and system developers should enable delegation of identity management limited to specific proxies and specific scopes (such as purposes, applications, data controllers, time etc.).

Delegate-Req: Data controllers, data processors, and system developers should enable revocation of delegation of identity management under defined conditions.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for a data subject to get an overview of decisions by her proxy regarding processing of personal data.

Delegate-Req: Data controllers, data processors, and system developers should provide concepts and mechanisms for identity management after one's death.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for issuance of the mandate of the proxy, invocation of actions under the name of the principal with the mandate, verification of the mandate, revocation of the mandate from the proxy and expression of acceptance of the mandate by the proxy.

Delegate-Req: Data controllers, data processors, and system developers should support derived credentials for proxies or that enable the proxy to use own credentials to get access and to act on behalf of the principal.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms that allow the principal to trace actions taken by the proxy.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms for the principle to declare preferences and conditions to the power of the proxy.

Delegate-Req: Data controllers, data processors, and system developers should provide mechanisms to maintain the proxy's private sphere

Delegate-Req: Data controllers should define how to deal with the data subject's data after her death. In particular, SNS providers should define and provide mechanisms for the user to determine the handling of profiles after her death.

Mech-Req: Data controllers, data processors, and system developers should develop, provide and use the appropriate IdM mechanisms for all parties involved in privacy-relevant data processing.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are accessible.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are effective, i.e., having the desired impact within a reasonable time frame with a reasonable effort.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are transparent concerning their potential impacts, limitations and side-effects.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are transparent concerning their effective impacts, limitations and side-effects.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing the appropriate IdM mechanisms are usable for the specific user group (for example, by well comprehensible user interfaces, limitation in complexity etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the devices bearing the IdM mechanisms have an appropriate security level (including hardware, operating system, software etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the management of (potentially) personal data has an appropriate security level concerning long-term storage, backup and recovery.

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, the appropriate IdM mechanisms will also work in a – due to long-term effects – potentially changed environment and prohibit lock-in risks (for example, by migration strategies, ensuring long-term portability where needed etc.).

Mech-Req: Data controllers (in particular application providers of IdM systems) should ensure that for all parties involved in privacy-relevant data processing, there are fallback solutions in case the appropriate IdM mechanisms fail or are not accessible.

IdM-Req: Developers of IdM systems and application providers should provide mechanisms to represent data such as attributes and attribute values in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should provide mechanisms to establish, evolve, and use partial identities from personal data such as attributes and attribute values.

IdM-Req: Developers of IdM systems and application providers should support third-party certification of attribute values of partial identities in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should support (privacy-enhancing) reputation systems in the user's identity management system.

IdM-Req: Developers of IdM systems and application providers should support authentication of actions w.r.t. partial identities.

IdM-Req: Developers of IdM systems and application providers should support the user in deciding which attributes and attribute values are revealed to whom.

IdM-Req: Developers of IdM systems and application providers should support users to store and make easily accessible the history which attributes and attribute values have been communicated to whom in which context.

IdM-Req: Developers of IdM systems and application providers should support delegation concerning all or specifically selected actions, contexts, and/or partial identities.

IdM-Req: Developers of IdM systems and application providers should support migration to other technologies, i.e., migration to other user devices and other communication infrastructure as well as use for new applications.

IdM-Req: Developers of IdM systems and application providers should maintain usability so that users can avoid errors as well as perceive their own digital life as continuous.

Transp-Req: Policy makers should define and explicate areas where revocable respectively irrevocable consequences are demanded respectively prohibited. This should guide system developers when conceptualising, designing and implementing ICT systems as well as application providers when operating applications.

Transp-Req: Policy makers and supervisory authorities should make clear what they demand from data controllers and data processors concerning privacy-relevant data processing, i.e., how to interpret privacy regulation.

DatMin-Req: Policy makers should support setting up and standardising the necessary infrastructure for issuing pseudonymous convertible credentials and their usage in their ICT systems where appropriate.

DatMin-Req: Policy makers should evaluate current legal provisions in the light of pseudonymous convertible credentials.

Control-Req: Policy makers should further limit exemptions to use (potentially) personal data for other purposes.

Control-Req: Policy makers should be extra cautious with (potentially) sensitive data.

Control-Req: Policy makers should rethink the concept of consent and possibly limit data processing based on consent in its scope or extent.

Control-Req: Policy makers should seek for ways to efficiently implement fair user control, easy to perform for all individuals.

Control-Req: Policy makers should revise the current framework for sanctioning privacy infringements and providing remedies for victims.

Control-Req: Supervisory authorities should sanction privacy infringements by noticeable punishments.

Control-Req: Policy makers should elaborate concepts for achieving remedy for victims of privacy infringements (“privacy infringement insurance”?).

Control-Req: Policy makers should propose guidelines for how to deal with conflicting policies.

Delegate-Req: For legally relevant settings, policy makers should regulate the circumstances of expressing and revoking delegation.

Delegate-Req: Policy makers should define general principles or guidelines for the handling of privacy by a proxy as an orientation.

Delegate-Req: Policy makers should provide rerequisites to enable later revision of privacy-relevant actions performed by the proxy on behalf of a data subject.

Delegate-Req: Policy makers should provide reasonable legal solutions to protect the proxy and to balance the interests of the proxy and the principal in a fair way.

ChangeMng-Req: Data controllers, data processors, system developers, and policy makers should monitor changes in society, law and technologies and react appropriately (for example, by evaluating chances and risks, adapting current processes, regulation or standards to the changed conditions etc.).

ChangeMng-Req: Policy makers should establish (privacy-enhancing) feedback mechanisms for society concerning privacy-relevant changes (for example, on attitudes what is to be considered private or public).

ChangeMng-Req: Policy makers should establish (privacy-enhancing) feedback mechanisms for society concerning privacy-relevant regulation, processes and technical implementations.

ChangeMng-Req: Policy makers should demand and support ex ante privacy assessments of technical, regulatory, and legislatory advancements.

ChangeMng-Req: Policy makers should consider the state-of-the-art and research results concerning privacy-enhancing technologies as well as potentially privacy-infringing technologies in law making, standardisation, funding and other supporting actions.