Analysis of Privacy and Identity Management throughout Life

Editors: Arnold Roosendaal (TILT)
Sandra Steinbrecher (TUD)
Ronald Leenes (TILT)
Hans Buitelaar (TILT)
Reviewers: Stuart Short (SAP)
Hans Hedbom (KAU)

Identifier: H1.3.3
Type: Heartbeat
Class: Public
Date: June 2009

Abstract

This heartbeat provides a thorough analysis of identity management in formal and informal settings throughout life. We discuss how identities are created, used, maintained, and terminated in these settings.

The formal key areas we cover are namely: government, education, healthcare, employment, and shopping. First, identity management here is approached at an abstract level, describing how a general formal identity is created. Then, identity management in the key areas is described. A more detailed overview for the first four key areas is provided from the perspectives of several European countries.

The example of informal settings we walk through are influenced by the social environment of individuals in their private life and cover the arising online applications that help people to interact with their social network. Here we point out the link to the other workpackages in Activity 1.

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.

SEVENTH FRAMEWORK PROGRAMME

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	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	Arnold Roosendaal (TILT)
First Chapter (Introduction)	Arnold Roosendaal (TILT)
Second Chapter (Identity)	Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD)
Third Chapter (Government)	Hans Hedbom (KAU), Stuart Short (SAP), Aleksandra Kuczerawy (K.U. Leuven), Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD)
Fourth Chapter (Education)	Aleksandra Kuczerawy (K.U. Leuven), Maren Raguse (ULD) Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD)
Fifth Chapter (Health Care)	Aleksandra Kuczerawy (K.U. Leuven), Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD)
Sixth Chapter (Employment)	Aleksandra Kuczerawy (K.U. Leuven), Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD)
Seventh Chapter (Social Networks)	Aleksandra Kuczerawy (K.U. Leuven), Arnold Roosendaal (TILT), Sandra Steinbrecher (TUD),
Overall editing	Ronald Leenes (TILT)

Executive Summary

This heartbeat gives an overview of privacy and identity management throughout life. Since this is a very broad scope, a choice was made to discuss privacy and identity management issues in four formal key areas in daily life. This discussion is first made at a general level, and subsequently specified for several European countries. After the formal identity part, there is an overview of issues in informal contexts.

Chapter 2 describes identity from a sociological and technical perspective. According to sociologist Goffman, identity is created in social interactions in different contexts. These contexts determine and shape the attributes and values that make up one's identity in that context. Information about individuals is represented in ICT systems. Records and files are commonly created containing information about citizens, customers, etc that are used for decision making and reference. The general nature of these representations, digital identities or digital personae, are briefly described. Clarke's distinction between projected digital personae, as created by the represented individual herself, and imposed digital personae, as created by institutions or other third parties plays an important role here.

In essence, individuals have one general formal identity which is not restricted to one specific context. Next to this general formal identity, formal identities in the various domains of (general) government (interactions), education, health care, and employment are described. Important issues are the existence of a unique identifier and the use of identifiers to establish connections between the context and the individual. In each of the domains the Heartbeat provides a a description of where data are collected and by whom.

The analysis (chapters 3-6) shows that in the Netherlands a unique identifier, the BSN, is commonly used in diffferent public sector settings. The BSN, in principle, allows for the construction of a compound identity, which provides detailed information about the individual across domains. In Germany this is not the case. There is even a separation between the different federal states, which all have their own regime in the various domains. However, all German citizens of age 16 and above are obliged to have a personal ID-card which is used for identification by public authorities. Up to now this card only plays a role in the physical world. The lack of 'globally' unique identifiers in Germany inhibits the creation of compound identities of German citizens. France and Austria both also have ID cards, but no unique identifier that is used throughout public services. Here, again domains are seperated through the use of different identifiers in each domain. Belgium, Sweden, Ireland, and Poland do use unique identification numbers, often combined with ID cards.

In the four formal areas, quite some differences occur. Some countries have national student cards, others do not. The same goes for electronic health cards. In the area of employment, all investigated countries turn out to have centralized systems to register unemployed people.

The chapter on informal identities (chapter 7) shows a number of issues that occur when it comes to lifetime aspects and identity management. The issues can be divided into three categories; data linking different persons; data about other persons, and; data about dead persons. Data remain available after decease. But already during ones lifetime, several problems occur because of the increasing (electronic) data exchange and processing, and because data is more often related to more than one person. Also, control is a specific issue, as can be seen in the case of minors or elderly, where control over data can be delegated to others, by law or on a voluntary basis.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This heartbeat aims at providing an overview of privacy and identity management issues throughout life. The topic will first be approached from a general point of view, describing where (formal) identities are established and what their functions are. The moment that a formal identity is created is usually at the birth of an individual. However, privacy and identity management related issues already take place before birth. During the future mother's pregnancy, files are created containing information on hereditary characteristics and the development of the foetus. Furthermore, information about the family of the unborn child is collected and insurances need to be taken out.

A similar process takes place after decease of an individual. Identity does not terminate immediately after death, but rather decays over time as rights and obligations terminate. For the purpose of pension funds and life insurances, the identity remains for a significant period. Besides, the personal details of the deceased person will remain accessible in municipal registers for historical purposes.

1.1 Privacy and Identity Management

This heartbeat is about privacy and identity management. Since this is a really broad concept, the focus is on formal identities of individuals. There is also more focus on the identity management aspect than on privacy aspects. These two concepts are closely related, but the idea is that identity management in formal contexts is a necessary condition for adequate protection of privacy of individuals. Keeping contexts separated and having control over what data are disclosed to whom can be facilitated by proper identity management, when different (partial) identities can be used for different contexts. Identities can differ depending on the contexts they are used in. For instance, specific aspects of one's identity may be more relevant than others according to the purpose and use of the formal identity.

In order to give a comprehensive overview of the relevance of formal identities and the management of these identities, four specific contexts in which formal identities play a role are described, namely government, health care, education, and employment.

Even though the focus is on formal identities –,described from the perspective of a number of EU countries –, there is also attention for informal identities to provide the entire spectrum of privacy

and identity management issues throughout life. Several domains are described and specific issues are touched upon.

1.2 Throughout Life

The four chosen key areas regarding formal identities describe identity management throughout life. It should be noted that the lifespan of a person's identity extends beyond their life. Wherever relevant, the identity establishment and use before life and after decease are therefore also described.

Furthermore, a number of questions arise when looking at identity and privacy from a lifespan perspective: How can a child after birth, a minor or a mentally challenged person manage their identities? How can they consent to collection or processing of information on their identity? How can a person delegate consent to such collection and processing, and still be “informed” as the law demands? How can we qualify the sensitivity of identity information from a balanced or fair perspective, when we are unable to ask the person(s) involved? The problems that arise are described in this Heartbeat. The current document serves as a starting point for other Heartbeats in WP1.3, and as an indication of the most relevant issues to be dealt with in the prototype.

1.3 Outline

This heartbeat first describes the creation, use, maintenance, and termination of formal identities in general (2). Next, these topics are described from the perspective of government, education, health care, and employment (3-6). In these descriptions, a more detailed overview will be given from the perspective of the Netherlands, Germany, Belgium, and Poland, and in a more limited form (due to resource limitations) from the perspectives of France, Austria, Ireland, and Sweden.

Chapter 7 gives an overview of specific issues concerning privacy and identity management in informal areas. Finally, chapter 8 draws some conclusions.

Chapter 2

Identity

This section describes the concept of identity. We will approach identity from a sociological as well as a technical perspective.

2.1 General Aspects of Identity

When talking about identity management, it is necessary to first have an idea of what identity is. This section briefly describes identity from both a social science and a technical perspective. It also discusses some concepts related to identities in the digital world.

Individuals interact with other individuals and organisations in many different relations, all of which are connected to different roles of the individual. Goffman defines identity as "the result of publicly validated performances, the sum of all roles played by the individual, rather than some innate quality."[1] In this respect, all different roles can be seen as (partial) identities.

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.

"Different (kinds of) relationships involve different kinds of information constituting the individual's identity. A single individual therefore consists of different characterisations tied to the different contexts in which she operates. For example, the co-workers in a work-related context will characterise an individual differently than the friends that interact with the same individual in the context of friendship. The relevant attributes associated to an individual are different in a working environment than in a social environment and individuals may also represent themselves differently throughout such contexts."[2] Some attributes may thus take different values in different context. For instance, James' nickname may be 'Jim' among his friends, whereas his colleagues might call him 'Captain Slow' (behind his back).

---

1 Goffman, Erving (1959). 'The Presentation of Self in Everyday Life', Doubleday Anchor Books, Garden City, New York.

2 PRIME Book (forthcoming) (2009 draft), p. 24.

Because different contexts impose different rules on behaviour and people play different roles (as in a theatre play) in different contexts and present different faces of themselves, we may say that individuals give different performances in everyday life. Audience segregation is at the same time a natural effect and an important enabler of the part one performs. "[B]y audience segregation the individual ensures that those before whom he plays one of his parts will not be the same individuals before whom he plays a different part in another setting."[3] Audience segregation is a device for protecting fostered impressions. Rachels states that this audience segregation "is an essential characteristic of modern (western) societies and allows for different kinds of social relationships to be established and maintained"[4]. If everyone has access to all information related to an individual all the time, relationships would no longer be possible. Figure 1 shows an example of an identity that contains several partial identities.

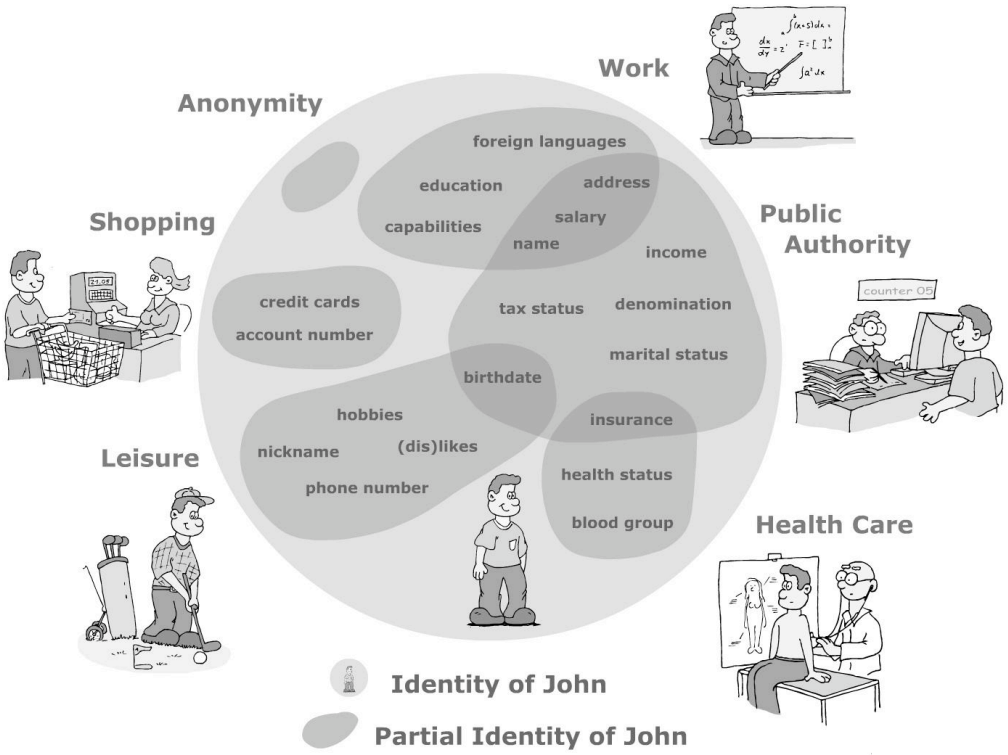

Figure 1: An identity comprised of multiple, different, identities.

Areas of life

Contexts can be grouped into areas of life as in Figure 1. 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.

Digital personae[5]

The establishment and maintenance of relations takes place offline as well as online. In the online context, representations of individuals (partial identities) can be referred to as 'digital personae' or digital partial identities.

---

3 Goffman, Erving (1959). 'The Presentation of Self in Everyday Life', Doubleday Anchor Books, Garden City, New York.

4 Rachels, James (1975). 'Why Privacy is Important'. In: *Philosophy and Public Affairs*, pp. 323-333.

5 The term personae is the plural form of persona. Some authors use personas as plural, however, we prefer the Latin form. Thus, the term 'personas' means the same as 'personae'.

Digital personae are (online) representations of individual's partial identities. This is, however, still a vague notion that needs further explanation. For this paper the starting point will be the definition of digital personae given by Roger Clarke: "The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual".[6] This definition clearly reflects the issue of representation. Furthermore, Clarke makes a distinction between projected digital personae and imposed digital personae. A **projected digital persona** is created by the individual and is strictly related to the way this individual wants to present himself. A MySpace profile page is a good example of this form. The individual has significant control over the image created by the audience. Users of Social Network Sites (SNS), of which MySpace is a well-known example, take great pains to construct and foster a certain image of their identity by means of typography, images, language, links, preferences, etc.

In contrast, an **imposed digital persona** is created by institutions based on the information they collect(ed) about an individual, and this persona has a certain function related to their task. Part of such a persona might be that Peter is unemployable because of his handicap, or that he is lonely and terminally ill. These images of his identity are likely not to be those that he himself would like to project to the world, but are rather the image created by the outside world and associated to him.
Recent examples in the Netherlands are the Personal Internet Page (Persoonlijke Internet Pagina, PIP) or the Electronic Child Database (Elektronisch Kind Dossier, EKD). However there are much older examples of imposed digital persona that are used since many decades such as estimating an individuals' creditworthiness, e.g. the Schufa in Germany.

Both projected and imposed personae have effects on the individual. People may find Helma a cool girl because of her MySpace profile, whereas her mother may judge her to be dull. Peter's environment will behave according to the persona imposed upon him by the various institutions. Based on digital representations, decisions are made, some of which are unknown to the affected individuals. However, the decisions clearly have an influence on these persons.

With regard to the projected persona and the imposed persona Clarke states: "The individual has some degree of control over a **projected persona**, but it is harder to influence **imposed personae** created by others. Each observer is likely to gather a different set of data about each individual they deal with, and hence to have a different gestalt impression of that person."[7]

The amount of data collected and stored about individuals is only growing. This is due to the difficulty, or impossibility even, to erase digital data. Once disclosed on the Internet, information will never again become private. This phenomenon contributes to the risk of collapsing contexts, i.e. separate contexts are connected or combined, when digital personae representing an individual are connected.

Lifespan

The lifespan of a human being is the range of time from the emergence of the first information that is related to this specific human being otherwise legally known as the data subject (a time period from the moment of birth until death or even thereafter) until the point in time when no more personal data is generated. Here, the verb 'generate' refers to new information becoming available to other persons than the former data subject. Hence, lifespan refers to the temporary aspects of privacy and identity-management and in particular to the challenges involved in realising (privacy-related) protection goals over very long periods of time. This aspect closely corresponds to the claim to cover identity management "from birth till death". Without going into unnecessary detail on ethical and philosophical questions about what constitutes human life, the lifespan broadly covers the time from the first diagnosis of a pregnancy until long after the data subject's

6 See: http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html (last visited: December 2008).
7 See: http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html (last visited: December 2008).

death. This is so because often times the estate of the dead reveals information about them. According to the Privacy Directive (95/46/EC), only data referring to a (living) natural person is considered "personal data", Art. 2. However, an individual may want to control how information concerning him will be treated after his death. With this definition, most lifespans will never end in theory (because one can never be sure that no more information will be found). But in practice one can consider an "information lifespan" over when the probability that such information will appear and, can univocally be attributed to the deceased individual becomes negligibly small. Another issue to take into account is that data concerning deceased people can contain information that is relevant for, or refers to, others, such as genetic data.

2.2 Identity in Formal Settings

In this section we describe the lifecycle of (partial) identities. There are a number of events related to the evolvement of the identity which can be described as different phases[8]:

- **"Establishing a partial identity"** means that the partial identity is created by or assigned to a person.
- **"Evolving a partial identity"** includes
    - the usage of the partial identity by the holder
    - the usage of a partial identity by others. Their maintenance includes observing or storing it and possibly by applying all kinds of data processing operations.
- **"Termination of a partial identity"** means deletion or suspension of the partial identity. Note that in some specific cases it can be possible to re-establish suspended partial identities.

All phases are relevant for formation of partial identities.

Identifiers

Personal identifiers are alpha-numeric strings that can unambiguosly be linked to a certain person. Such a personal identifier may be created for the whole lifetime or even beyond (e.g. in Germany a number created for the pension insurance fund that may also pay to an insurant's wife).

"All [EU] countries use general identifiers that are not restricted to use within one specific application or sector. Such identifiers would in principle be more suitable for identification purposes than sector/application specific sectors, since they are less likely to be restricted to a limited user group. However, in some countries their use is restricted by law, precisely in order to avoid that governments can link personal data about a specific person across different sectors, which is considered to be a privacy threat in some countries. This can render them unusable for cross border authentication purposes."[9]

Formal Identities

The establishment and use of formal identities usually takes place by institutions. They create, on the basis of a legal obligation, an identity or identifier. Data about individuals related to the specific context or purpose of the identifier is connected to the identifier. All together, the sets of data form partial identities.

Our general formal identity is given or created by the state. When a child is born, the parents have to register the child at the governmental institution of the place of birth. When the child is

---

8 Hansen, Marit/Pfitzmann, Andreas/Steinbrecher, Sandra (2008). Identity Management throughout one's whole life, Information Security Technical Report (ISTR) Vol. 13, No. 2 (2008); Elsevier Ltd, Cambridge (UK); 83-94.

9 IDABC (2007), Analysis and Assessment Impact Report, v. 3 5, p. 37.

registered, the government provides a formal identity in the sense that there is a record of birth made up. This record contains the name(s) of the child, date of birth, place of birth, and information about the parents. The child will also receive some unique identifiers, usually numbers. For instance, in Germany the number of the birth certificate is one identifier, and the newborn is also assigned a unique number for tax purposes whilst in the Netherlands, the newborn receives a BSN, which is used in multiple public sector contexts.

The name(s) of a child are chosen by its parents, but formally it is often the state that assigns the name to the child and therefore it is the state which creates the newborn's identity in the formal sense. There are restrictions on first names to be proposed for the newborn. Some trade marks or sensitive names (from a historical perspective or because they are immoral) will be refused by the authorities. Famous in this respect is the French case regarding the parents who wanted to name their little girl Mégane Renauld pronounced the same as Renault Mégane, a popular French car at the time. Although the courts ultimately decided not to overrule the parents, they could have done so.[10]

With regard to the family name, the child receives the name of its father or/and mother (in the Netherlands at least the parents can choose which family name their hild receives). Married parents in Germany either already have settled for a family name when they married, which automatically transfers to their children, or the parents have to select one of theirs to transfer when the first child is born. The chosen family name is given to all following children. If the parents are not married, the name of the mother is given by default if the mother does not declare that she wants the name of the father to be given. An interesting complication arises when the unmarried couple decides to marry after the child's birth and decide to adopt the father's surname as the family name, because then the child's surname will change as well. Also more complicated naming schemes exist. In Spain, for instance, children receive both their mother's and father's surname and hence have a double family name. In Ireland the parents decide on the family name of the child when registering the birth and may change this at a later stage; there is no restriction on using composed family names.

Not only names of children may change over time. In many countries it is customary or even a legal obligation that married women acquire their husbands name when they marry. Also individuals may request a formal name change, due to, for example, harassment, cultural issues (for instance, in the US many immigrants have requested name changes to better blend into the US culture[11]), or witness protection schemes. In other words, names are not particularly stable identifiers for individuals, which is one of the reasons for the popularity of numbers as identifiers in formal contexts.

The unique identifiers (the numbers) given will, usually, be used throughout the individual's entire life in interactions with the government. These interactions include for instance taxes and subsidies as well as the distribution of travel documents (passport) or identity cards and driving licenses.

The information will be kept in the official registers: "data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal or factual trust is attached (i.e. which are generally assumed to be correct)"[12]. The identity information can be kept in municipal administrations, local

---

10 See Whitman, James Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty, 113 *Yale L.J.* 1151 at 1217, available at http://ssrn.com/abstract=476041. (citing CA Rennes, 6e ch., May 4, 2000, J.C.P. 2001, IV, 2655, note Pierre & Boizard). "The court's opinion emphasized that the parents had not any 'arrières-pensées'—that is, any unacknowledged or ulterior intentions, and that the car model in question would likely go out of production by the time the child reached school age."

11 See Scassa, Teresa (1996). National Identity, Ethnic Surnames and the State, 11 *Canadian Journal of Law and Society* 167.

12 Definition token from: IDABC (2007). Analysis and Assessment Impact Report, v. 3 5, p. 54.

records, as well as at a central governmental level. If a person moves from one city to another city, he generally has to deregister in his old hometown and register in the new one.

After decease, a death certificate is created and the death is registered in the local records. The data remain archived for, amongst others, genealogy and statistic purposes.

2.3 Formal Identities in Different Contexts

Next to the general formal identity as described above, a number of context-related partial identities are created during the lifetime of the individual. This section describes these identities in four key areas of life, namely government, education, healthcare, and employment.

2.3.1 Government

Soon after the birth of an individual, the government grants a birth certificate and thus creates the identity of the individual for governmental registries. Probably, the certificate also contains a number or other identifier which is then connected to the individual. From then on, identification of the individual takes place on the basis of this number. Next to interactions between the government and the individual, other interactions may use the same identifying number. Many interactions with the government leave traces in the individual's records.

Termination of the identity takes place after death. However, this only counts for the identifier, in as far as the number will be 'decommissioned' and will be placed on a revocation list. The records remain, together with the registries.

City administration records also contain information on the date of birth of an individual and its marital status. In tax filings, this information is combined with information on income and some insurance. Usually, tax filings use the same identifier as provided by the government at birth.

Once an individual dies, the information is used to identify the heirs and to get all administrations correct.

As described above, the government creates a general formal identity for each individual. However, next to this general identity there may be many partial identities, related to specific contexts. These identities can be separated, but may be connected via the general identifiers of the individual. In the governmental domain driving licenses, travel documents, taxes and subsidies were already mentioned as specific contexts. These smaller contexts all have their own identity information concerning the individual. Other examples are marriage, changes in family situation and permits for building or parking.

2.3.2 Education

Another important context where a partial identity is used is the educational domain. In principle, all individuals go to school at some point in time and many go to kindergarten before entering a school career. In kindergarten, as well as in school, records are created on the (social) development of the child.

Once an individual starts visiting school an identity will be created by the school. Probably, only name and address details together with date of birth are used to directly identify a person, whereas additional data on personal development give a more profound view of the individual. However, it is more likely that the educational institution also creates an identifying number which is used to indicate an individual. During the educational life-cycle, data about grades and certificates, personal comments from teachers, and general observation data are added to the records, thereby shaping the pupil's or student's identity. Most educational institutions use electronic systems with

pre-fixed tables and schemes to describe the development of the child. Not only skills such as writing and counting are included, but also social skills such as “How does the child react to the teacher/strangers?”; “Can the child play/work on his own?”; “Does the child have many friends?” etc.

Usually personal data on the individual and possibly his relatives (e.g. parents, brothers or sisters) are disclosed to the school, and the way how to prove the authorisation for attending the courses is communicated – e.g., by simply stating one’s name or by showing an assigned chipcard. As soon as these partial identities are created and the individual himself begins to use them like by attending school, he begins to further develop those partial identities – and thereby also to manage identity – himself.

Files regarding education will contain personal info and grades as well as an overview of which education someone follows. When the age of the individual and his/her educational level are rising, files will also contain information about financial support and whether a student is living with his/her parents or not.

Occasionally, data will be shared amongst different educational institutions, for instance when someone switches to another school or goes from secondary education to a university. At least diplomas will be needed, but probably also grade lists and other information. This information might be exchanged either directly between the different educational institutions or the individual gets a certificate from the first institution that he shows to the second institution.

When an individual finally finishes education, the partial identity could be terminated. However, diploma or certificate information remains stored in order to be able to verify the authenticity, implying that the identity is maintained and remains.

Student records give an insight in the number of students and the kind of students someone is studying with and they have an index of registered certificates. The registration of these certificates can be shared with other instances than the school itself, for instance when there is a verification needed.

It is also possible that schools collect information on extra curricular activities of their students.

2.3.3 Health care

Prior to the newborn’s birth, data will be collected from the mother-to-be and the pregnancy that will become part of the newborn’s identity. Peculiarities during the pregnancy and certain developmental or genetic defects will be recorded and become part of the medical record that is created at the child’s birth. Before and after birth, general practitioners, specialists, hospitals and other health care professionals exchange patient and medical information. Some of this information will also be shared with health insurance companies (think of treatment bills) in order to be able to conclude insurance policies. Medical data may also be collected by research institutes and government agencies for epidemiological surveys. In these cases the data usually will be anonymised.

From an early stage, records are kept on vaccination and blood group. Depending on the events that occur during someone’s life, extensive medical records may develop. Furthermore, Health care during someone’s life can include somatic health care as well as mental health care.

2.3.4 Employment

In order to get employed, people need to have a social security number (provided by the government or tax services). Employers will create a file which includes information on name and

address, educational level, kind of work, a complete CV, and salaries or wages. Probably, the employee also gets an employee number from his company.

Capabilities will be tested and there is information about the function and status of an individual (employee/employer, freelancer, etc.).

Identity management related to employment includes both the situation of being employed and being unemployed. Once an individual becomes unemployed, he may apply for social security and will probably be registered as job-seeker. There can be a duty to apply for jobs, which is supervised by the government.

2.4 Identities and social networks

Typically people do not live alone and independent for the whole of their life; they start with parents, some will marry and have children and grandchildren. Usually many other relatives exist; ones they know about, others they are nor aware of. Most people also have a number of friends, schoolmates, and colleagues during their life. Although schoolmates are people one gets to know at school and colleagues are people one gets to know at work, usually the link to them can not be described formally. The social network people form and live in nevertheless affects their privacy as much or even more than the formal areas described above. This holds even more nowadays in the time of Web 2.0 because many people transfer their real social network to social networking software and begin to form new social networks on the Internet. Often they are not aware of the fact that the people they address with postings on a web site are not only friends, but often include every user on the world with Internet access.

In this heartbeat we concentrate on the following aspects of social networks that affect someone's privacy (also in the formal areas) and may result in persons with the inability to protect themselves against privacy breaches:

- Data belonging to more than one person
- Data about other persons
- Data about dead persons

Chapter 3

Identity and Government

3.1 The Netherlands

Formal identities are provided by the state and issued by the municipalities. Official ID documents are: identity card, passport and driver's license.[13] These documents are based on the information present in the Municipal Registry, which e.g. contains name, last name, address, gender, marital status, nationality, administration numbers and citizen service number, and information concerning parents, partner and children.

Electronic identities are provided and governed by DigiD, the common authentication system for government institutions, run by 'GBO.overheid'. GBO.overheid is a division of the Ministry of Interior and Kingdom Relations. Next to the GBO.Overheid initiative, the Dutch eGovernment landscape comprises over 40 organisations and projects.[14]

In the Netherlands, the *Burger Service Nummer* (Citizen Service Number, BSN) is used to identify individuals and allow them to perform transactions with governmental institutions. "Obviously, the Citizen Service Number is meant to facilitate the communication between governments and citizens, but may be used by companies under certain conditions. Already in place at the moment is the so-called DigiD. DigiD stands for Digital Identity and is a system shared between cooperating governmental agencies, allowing to digitally authenticate the identity of a person who applies for a transaction service via internet. With increasing numbers of public authority offices implementing the DigiD system, it is easy to begin using their range of electronic services after first choosing your own login code (user's name and password) at www.DigiD.nl. In short: DigiD provides users with a personalised login code for the full spectrum of contact with various governmental bodies."[15] In technical terms this is called 'single sign-on'. Anyone with a Citizen Service Number can apply for a DigiD.

The DigiD service comprises three assurance levels and hence three different kinds of DigiD's can be obtained by the claimant. The first and second assurance levels are called 'DigiD basic' and 'DigiD middle'. The third level, 'DigiD high', will be filled in by the Dutch electronic Identity Card 'eNIK', which is currently under construction.

A model of the DigiD scheme is provided in Figure 2.

---

13 Based on the 'Wet identificatieplicht 2005' (Identification Act).

14 http://www.e-overheid.nl/e-overheid/projecten/projecten.html (last visited: December 2008).

15 IDABC (2007). eID Interoperability for PEGS, National Profile The Netherlands, p. 9.

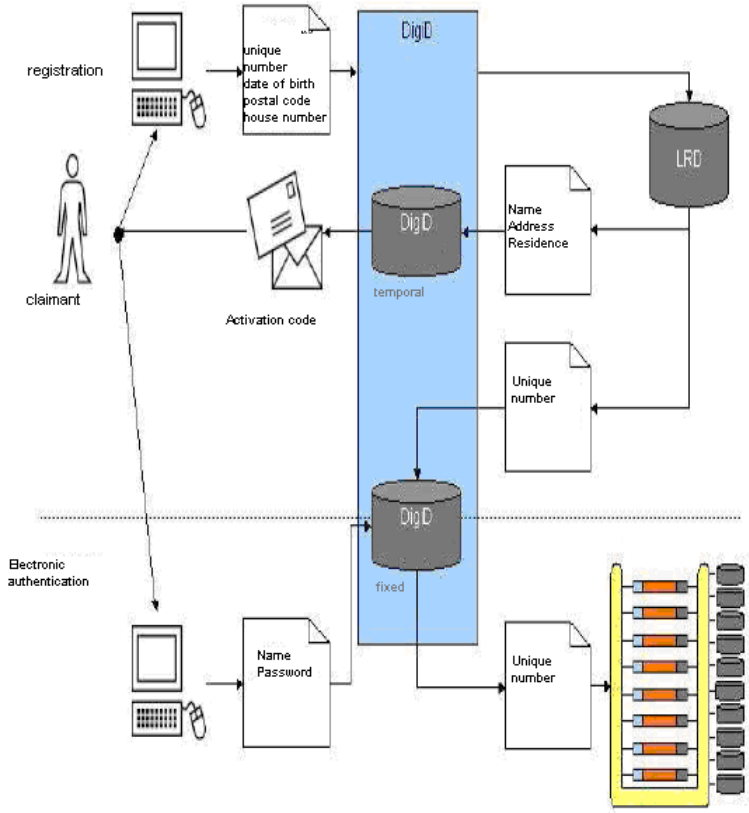

Figure 2: The DigiD scheme (www.digid.nl)

3.1.1 Attributes

The Dutch eID model consists of a very shallow digital identity, the BSN. This 'gloabbly' unique identifier is the linking pin to a large number of public sector databases[16] that comprise data about the individual. Important databases in this respect are the authentic registries, such as the Municipal Registry, which contain certified (and official) information and which should be consulted by public sector entities whenever data about the citizen is required. The Municipal Registry contains information about residents in a municipality, such as name, last name, marital status, address, residence, parents and children. The Municipal Registry is governed by the Act of 9 June 1994 on the Municipality Basic Administration. There are nine other authentic registries in the Netherlands.

The citizen can authenticate himself in electronic transactions with his DigiD, which offers the relying party (an e-Gov service) the citizen's BSN upon successful authentication.[17]

Everyone who engages in relations with the Dutch government (and thus also persons that stay in the Netherlands for a longer time or work in the Netherlands) is granted a BSN. The BSN has replaced the Dutch Social-Fiscal ('SoFI') number in November 2007. It is the single identifying number used in all citizen-government relations. Traditionally, public sector institutions use/used

16 The BSN is also part of many private sector databases, employers for instance have the BSN for tax purposes. The private sector may not use the BSN as an identifying number on the basis of the current legislation.

17 Cf. Buitelaar in FIDIS Deliverable 16.1.

their own identifiers, such as a healthcare number, a student number, a social-fiscal number, and an 'A-number' (the identifier used in the administration). Many of these are replaced by the BSN.

The BSN (9-digits) does not contain any personal information.[18] Section 8 of the Act on the *Burger Service Nummer* states that the body of burgomaster and alderman assigns the *Burger Service Nummer* to an individual immediately after registration in the Municipal Register. The Act on the Citizen Service number defines that only 'users' are allowed to use the Citizen Service Number. 'Users' are defined as administrative bodies (Article 1d(1) Act on the Citizen Service Number), or any other to which the use of a Citizen Service Number is prescribed by law (Article 1s(2)). For example, an employer may use the number for limited purposes, for instance for tax purposes, but not as a general employee number. The use of the *Burger Service Nummer* in the health care domain is regulated in the 'Act on the use of the Citizen Service Number in Health Care'. The use of the BSN is therefore restricted.

3.1.2 Establishment and Termination

The eID (DigiD) is issued upon verification of the information provided by a webform application, against the information that is recorded in the Municipal Registry. After verification, the applicant will receive an activation code by regular mail on the address associated to their BSN according to the Municipal Registry. The applicant subsequently has to activate his DigiD by entering the activation code on the DigiD website. This is a relatively light enrolment procedure.

Termination of the Digital Identity can be done by the identity provider (GBO.overheid), at all times,[19] which is also the case for a claimant who wishes to delete his or her DigiD at the DigiD website.[20]

3.2 Germany

Unique and universal personal identifiers (Personenkennzeichen) that are valid for a whole lifetime can be used to build large personal profiles. For this reason the German Federal Constitutional Court (Bundesverfassungsgericht) declared in the Mikrozensusentscheidung[21] in 1969 that personal profiles built without giving the person concerned the possibility to verify the correctness and usage are illegal. This judgement was confirmed in the Volkszählungsurteil of 1983.

For this reason there is no universal personal identifier in Germany but there are only sector-specific identifiers. For a long time the sector-specific identifiers have only been used for a certain time frame. This is changing for security reasons. In many sectors there is an urge to create life-long personal identifiers at least for the sector.

Identity management systems applied to the various sectors, and maybe even interoperable between sectors, have to be able to work without universal personal identifiers as a result of the 1983 Court ruling. In the following section, the development in the creation of personal numbers in the four key areas in Germany will be described. Parts of this description have already been presented in German.[22]

---

18 S. 2, Act on the Citizen Service Number.

19 S. 8 general terms of use DigiD, see: http://www.digid.nl/privacy/ (last visited: December 2008).

20 S. 2(17) general terms of use DigiD.

21 BVerfGE 27, 1 = NJW 1969, 1707.

22 Hansen, Marit/Meissner, Sebastian (Eds.) (2007). Verkettung digitaler Identitäten, ISBN 3000234063, https://www.datenschutzzentrum.de/projekte/verkettung/ (last visited: December 2008)

3.2.1 Registers

In Germany there are a number of governmental registers, the most important ones being the register of registration (Melderegister), the register of ID cards (Personalausweisregister), the register of passports (Passregister), the registers of civil status (Personenstandsbücher)[23], the cadastral registers (Grundbücher), the register of driving licenses (Führerscheinkartei), the Federal Central Criminal Register (Bundeszentralregister), the Central Register of Traffic Offenders (Verkehrszentralregister), the central register of vehicles (Fahrzeugregister), the commercial register (Handelsregister), the central register of companies (Gewerbezentralregister), the register of associations (Vereinsregister) and the central register of foreigners (Ausländerzentralregister).

In the following details of the Melderegister are given.

The Melderegister should allow both identification of residents and their place of residence (identification function) and provide information to governmental and private institutions (information function).

The legal foundation of the Melderegister is the Melderechtsrahmengesetz (MRRG) and the Meldegesetze of the German Federal States. Future legislation in this area will be given with a Bundesmeldegesetz as agreed in the Föderalismusreform 2006, but still to be agreed on and enacted. The execution of these laws shall be administered by the German Federal States and its communal registry offices (Meldebehörden)[24] for the residents in their administrative district. The Melderegister in the Meldebehörden should fulfill the identification and information function. The data contained in a Melderegister might either be collected from the persons concerned, or might be transmitted by administration authorities, or might have become known officially[25]. The completeness and correctness of the Melderegister is guaranteed by official updates, evidences from other administration authorities (Fortschreibung von Amts wegen und Hinweise öffentlicher Stellen) that received data from registers and the general compulsory registration obligation for citizens (allgemeine Meldepflicht)[26].

In the Melderegister the data listed in Table 1 should be contained (including proofs of its correctness).

---

23 From 01.01.2009 till 31.12.2013 the former Personenstandsbücher in paper form will be transferred to a digital register. The legal basis for this is the Personenstandsrechtsreformgesetz from 2006 (published 23.02.2007 in Bundesgesetzblatt).

24 Art. 83 f. GG.

25 § 1 Abs. 1 S. 4 MRRG.

26 Vgl. §§ 4a (Fortschreibung von Amts wegen und Hinweise öffentlicher Stellen) and 11 (allgemeine Meldepflicht) MRRG.

Data in the Melderegister		
Last name	Prior names	First names
Doctoral degree	Religious name or pseudonym	Date and place of birth
Gender	Legal representative	Nationality
Legal membership in a religious group	Current and prior addresses, main residence, secondary residence,	When moving from abroad to Germany the prior address in Germany
Date of moving out or in	Family status	Spouse or life partner
Minor children	Issuing authority, issuing date, period of validity, serial number of the passport/ ID card.	
Forwarding block (Übermittlungssperre)	Date and place of death	If applicable additional data

Table 1: Data in the 'Melderegister' (1)

Additionally the data listed in table 2 (Melderegister 2) can be contained to realise additional purposes.

Data in the Melderegister (2)		
Data for preparing European or German Parliament elections	Data for issuing income tax cards	Data for issuing ID cards and passports
Data for legal processes concerning nationality	Data for tracing services (Bundesvertriebenengesetz)	Data for legal processes concerning weapons law
Data for unambiguous identification of residents concerning taxation (tax ID number)		Data for legal processes concerning explosive law

Table 2: Data in the 'Melderegister' (2)

The German federal states may decide to store additional data.

In the context of the Bundesmeldegesetz, the current German Government plans a central register of registration[27].

3.2.2 Identification

Both paper based and electronic ID documents exist in Germany. Paper-based ID documents, such as the passport, may also contain a machine readable area. The current ID card (Personalausweis) is paper-based, but the future ID card will be an electronic ID document similar to the passport and the existing electronic signature card.

The purpose of the **passport** is the identification of German citizens abroad. The passports have to be shown not only at the border but also e.g. in hotels and maybe also delivered to others for a short period of time (e.g., up until two hours in Italy, up until eight hours in Slovakia).[28] Legal

[27] "Bericht: Bundesregierung plant zentrales Melderegister" http://www.heise.de/newsticker/meldung/83859/ (last visited: December 2008).

[28] Meints, Martin/Hansen, Marit (Eds.) (2006). FIDIS Deliverable 3.6 – Study on ID Documents, Version 1.1, Frankfurt am Main; http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf (last visited: December 2008).

foundation for the technical implementation of the passport is EU Directive 2252/2004 and the German Passgesetz, which both refer to the International Civil Aviation Organisation (ICAO) specification for machine readable travel documents.

The passport is realised as a card with polycarbonate lamination containing the personal data and nationality of the passport owner and the issuing authority. Additionally the card has an area readable with optical scanners and character recognition („machine readable zone", MRZ) that contains the passport holder's name and date of birth, the passport number and the period of validity.

Passports issued since November 2005, also contain an RFID chip, that digitally stores the passport holder's personal data and a digital photo of his face that can be used for face recognition. On passports issued since November 2007, also photos of two finger prints are stored digitally on this chip.

The purpose of the **ID card (Personalausweis)** is the identification of citizens by public authorities. The legal basis for the card is the Personalausweisgesetz. All German citizens over 15 need to possess an ID card. Citizens need not carry the ID card at all times, but they must be able to show it to public authorities on demand. The ID card is also used in the commercial area to e.g. verify a customer's age.

In the future the ID card should have similar technical features as the passport (RFID chip and biometric data) and a chip for storage of keys and certificates for electronic signatures.[29]

The purpose of **electronic signature cards** is the storage of private keys and certificates needed for electronic signatures. The legal basis for the card are the Signaturgesetz and the Signaturverordnung. In Germany signature cards are issued by private service providers on the basis of legal foundations (which are based on the EU eSignature Directive 1999/93/EC). The Public-Key Infrastructure (PKI) needed for verification of the data on signature cards is also provided by private service providers, and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI).

For every electronic signature the certificate in the form of an X.509v3 certificate of the owner is stored on the card. The certificate contains an unambiguous certificate number, the name of the owner and his private key's period of validity.

3.2.3 Taxation identifiers

For a long time German residents only received a tax number when they requested an income card for their first job, which usually did not happen before reaching majority age. Whenever the individual moved to another commune, his tax number changed. When people married both partners received the husband's tax number as the number to use in the future by both.

With the introduction of the new tax number, which is legally based on §§ 139a ff. of the Abgabenordnung (AO) and whose distribution to the residents started in July 2008, a new uniform and unchangeable identification number for natural persons is created. Every resident gets this number independent of age. Tax authorities use this number to identify each resident unambiguously. This means that every other authority involved in an individual's activities that might be subject to taxation also have to know and store the individual's tax number to show it to tax authorities.

The tax number is issued by a central authority, the Bundeszentralamt für Steuern (BZSt). BZSt communicates with the communal registry offices to exchange data about the residents. The

[29] Engel, Christian (2006). Auf dem Weg zum elektronischen Personalausweis – Der elektronische Personalausweis (ePA) als universelles Identifikationsdokument, in: Datenschutz und Datensicherheit (DuD), S. 207 ff.

communal registry office sends personal data about a resident e.g., name, date and place of birth, address. And the BZSt in turn sends the tax number. Both authorities store all data created and received.

The tax number consists of 11 digits that should not be deducible from other personal data, cp. Table 3:

Digit	Content / Meaning	Example
1-10	11 digits	1234567890
11	check sum	1

Table 3: New tax number in Germany

According to § 139b AO the tax number is only allowed to be used for taxation to prevent the creation of one unique personal identifier.

3.3 Belgium

3.3.1 The National Register[30]

In Belgium, information about natural persons (Belgian citizens) staying within Belgian borders, natural persons without Belgian nationality and those who await for the decision (like refugees)[31], is kept by the National Register.[32] It is a national database which is kept up-to-date based on registers managed at the communal level. The creation of the National Register started in 1963 and was completed in 1983 when the Law of 8th August 1983 establishing a National Register on natural persons[33] came into force. The law has been updated several times since.

The National Register contains information for all persons included in the population registers, the non-nationals registers and the waiting registers. For each of these persons, the National Register contains: last and first names, date and place of birth, gender, nationality, main place of residence, place and date of death, occupation, marital status, family composition, source register, administrative status of persons in the waiting register[34], reference to identity cards (electronic or classic), and legal cohabitation. All changes to this information must be notified from the date from which it has legal effect. Information is kept until 30 years after the date of death. Access to the information in the National Register is restricted and the list of entities that have access to the Register is provided in the Law establishing a National Register.

The National Register uses the INSZ-number, which is the identification number for social security services. This number uniquely identifies people known to the national register or to the BIS register. Its composition is: YY.MM.DD XXX-XX, where YY.MM.DD signifies date of birth of the holder and XXX-XX a serial number.

Depending on the status of the individual, information about them is first entered into these databases based on particular legal situations that give grounds to such registration. The most

30 This part is based on: J. DUMORTIER and H. GRAUX, 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, November 2007, p. 17-18, available at: www.epractice.eu/resource/2056

31 The information about non-Belgian citizens is kept in the BIS register. This has the same functionality as the national register, but holds information on this category of people.

32 Het Rijksregister/Régistre national;

33 Law of 8 of August 1983 establishing a National Register on natural persons, Belgian Official Journal 21 April 1984;

34 Information like: asylum requested, asylum rejected – appeal pending, etc.;

common possibilities are: registration at birth, naturalisation or asylum requests and/or decisions (which are reported to the communes by the competent authorities), and official notifications of changes of domicile by the person involved at his commune.

The traditional identity infrastructure "consists of centrally kept but locally maintained paper registers for natural persons and of an identity card to certain natural persons".[35]

Moreover, it should be mentioned that the Law of 25th March 2003 modifying the law of 8th August 1983 establishing a National Register of natural persons and the law of 19th July 1991 regarding the population registers and identity cards and modifying the law of 8th August 1983 establishing a National Registry of natural persons, modernized these existing registers, in a way that established them as an authentic source for electronic identity data.

3.3.2 Crossroads Bank for Social Security

The main goal of the Crossroads Bank for Social Security (CBSS), created in 1991, is the stimulation and co-ordination of eGovernment in Belgium.[36] Apart from co-ordinating and facilitating electronic data exchange between actors of the social sector, the CBSS actually organizes these data exchanges. To achieve this, the CBSS runs a 'reference directory', which displays information[37] about: 1) which persons/companies have files at which entity of the social sector for which periods of time, and in which capacity they are registered ('directory of persons'); 2) which information/services are available at which entities of the social sector ('data availability table'); 3) what kind of information/service can be accessed, in what situation and for what period of time ('access authorization table'); and 4) which users/applications wish to receive which services automatically.

The purpose of such reference directory is to[38]: 1) route data requests to entities that can supply the requested data; 2) transmit data automatically where appropriate (e.g., change in address); and 3) to perform access control.

It is worth mentioning that the CBSS has a direct connection to the National Registry.

The CBSS reference directory does not contain personal data. It only contains 'pointers' that allow locating and retrieving the information.[39] Personal data is referenced using the 'INSZ-number' (either the National Registry Number for all persons who are registered there, or an identification number provided by the Crossroads Bank itself[40]) of the person to whom the data refers.

Aside from the reference directory the CBSS collects and maintains additionally certain identity information itself (e.g. its own repository of identity data contained in the National Registry and a

---

35 J. DUMORTIER and H. GRAUX, 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, November 2007, p. 17-18, available at www.epractice.eu/resource/2056, p. 14;

36 D. DE BOT, ''Privacybescherming bij e-government in België. Een kritische analyse van het Rijksregister, de Kruispuntbank van Ondernemingen en de elektronische identiteitskaart als belangrijkste juridische bouwstenen', Brugge, Vandenbroele, 2005, p. 77.

37 Crossroads Bank for Social Security, 'e-Government Program of the Belgian Social Sector', December 2008, published at http://www.ksz.fgov.be/documentation/En/CBSS_2008.pdf, p. 5; F. ROBBEN and P. MAES, 'De Kruispuntbank van de Sociale Zekerheid als motor van E-Government in de sociale sector', 2006, available at http://www.ksz-bcss.fgov.be/documentation/nl/documentation/Pers/De_KSZ_in_2006.pdf p. 7 and http://www.ksz-bcss.fgov.be/nl/fluxdonnees/fluxdonnees_2.htm.

38 'E-Government in the Belgian social security sector – Belgian Best Practices', 2003, available at http://www.ksz-bcss.fgov.be/en/como/brochure%20definitief.pdf, p.12

39 J. DUMORTIER and H. GRAUX, 'eID interoperability for PEGS – National Profile Belgium', report for the IDABC study on European eGovernment Services, November 2007, p. 17-18, available at www.epractice.eu/resource/2056;

40 For those in the BIS register.

Register with similar identity data for persons not listed in the National Registry, but who receive social security in Belgium).[41]

The authorization of users is based on a 'generic Policy Enforcement Model', complementary to the access authorization table. Requests for access or to perform a particular action, together with the relevant information concerning the request (identification of the user, requested information, context) are being assessed and the answer is given whether or not the user is authorized to perform the requested action. The decision is based on the policy rules, which describe under which conditions authorization may be granted.

3.3.3 eID

The Belgian eID Card is a smartcard with an embedded chip. It was introduced in Belgium in 2003 and since 2009 all the citizens from the age of 12 should be in possession of such document.

The Belgian eID is a classic smartcard, using traditional public-key technology where the private keys are generated in the card and the corresponding public keys are protected with a public-key certificate.[42] Currently there are three types of electronic identity cards issued: Belgian eID cards, Kids-ID cards, and foreigners' eID cards.[43] Each consists of the same chip with identical functionalities, however they do not all contain the same certificate types.[44] A Belgian eID supports three electronic applications allowing for: 1) digital identification of the card holder; the production of 2) authentication and 3) qualified electronic signatures. Additionally the card provides one non-electronic function which allows for 4) ordinary visual identification of the card holder.[45]

The card contains two types of information: visible and invisible. Visible information contains all the names, the nationality, the place and date of birth, the gender, the place of delivery of the card, the begin and end date of validity of the card, the denomination and number of the card, the photo of the holder, the signature of the holder, and the identification number of the National Register. The invisible information contained on the chip is the same information as on the visible type, plus identity and signature keys, the identity and signature certificates, the accredited certification service provider, information necessary for authentication of the card and protection of the electronic data, and the main residence of the holder. Currently no encryption certificates, no biometric data[46], no electronic purse, no storage of other data is available.

The card is expected to become the main authentication instrument for accessing e-government services in Belgium. The goal is the generalization of use of eID in most applications such as paying invoices online, sending registered electronic mail, filling in the annual tax declaration (in use), accessing personal files (Dossiers) held by the National Register (in use), e-procurement, or verifying residences of recipients receiving registered mail at the Post Office.[47]

---

41 Art. 4 of the Law of 15 January 1990 creating and Organizing a Crossroads Bank for Social Security (Belgian Official Journal, 22 February 1990). See also http://www.ksz-bcss.fgov.be/Nl/fluxdonnees/fluxdonnees_4.htm;

42 B. Van Alsenoy, D. De Cock, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit, 3/2008, pp. 178 – 183.

43 B. Van Alsenoy, D. De Cock, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit, 3/2008, pp. 178 – 183.

44 A Kids-ID issued to children under six does not hold any certificate. For more information on the Kid's ID card visit http://www.ibz.rrn.fgov.be/index.php?id=564&L=1.

45 B. Van Alsenoy, D. De Cock, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit, 3/2008, pp. 178 – 183.

46 Only the picture is stored for 'traditional' human inspection, but no separate fingerprints or iris scans.

47 Electronic ID Card: Belgium Implements Affordable Digital ID Cards, available at: http://be.country.csc.com/en/cs/2789.shtml

The Government expects that, over the years, both the public and the private sectors will make a wealth of additional applications and services compatible with the eID card.[48] In order to achieve this, the card contains relevant data for such extended uses.

The critics of the Belgian e-ID say it provides strong security against traditional outsider attacks, but unfortunately it has not been designed with privacy in mind.[49] The two main accusations are: the fact that national registry number is the regulated identifier, and the unrestricted access to the data file.[50]

3.3.4 The life cycle

Birth and before: In Belgium the foetus is not considered as a legal subject, only living people are. The protection as a legal subject starts at the time of birth, when the child is alive and viable and not at time the foetus is conceived. Every living person has rights and obligations, but not necessary *full* (art. 18 Belgian Constitution). Once the child is considered as a legal subject, some retroactive rights are assigned, so a conceived child can hold certain rights as long as it is alive and viable at the time of birth. This goes back until the "legal" moment of conceiving but can only be an advantage for the foetus itself and not for a third person like the mother (art. 725 and 906 Civil Code). The law provides a presumption of the moment of conception since it is not externally visible. Each child is presumed to be conceived between 300 and 180 days before the day of birth, but it is allowed to prove that the foetus was conceived earlier. Within this time period it is presumed that the baby could be conceived on every chosen moment (*omni meliore momento*) (art. 326 Civil Code). Therefore each foetus will be able to claim all rights of the facts which happened in this 121-day time-period, e.g. the child will have the right to compensation. However, this rule functions only within civil law; the rules are different for criminal law. In case of data protection, under the Belgian Data Protection Act,[51] the data about unborn children are *sensu stricto* not personal data since they are only becoming a person once they are born. It should be noted that according to art. 4.5 of the Council of Europe's Recommendation No. (97)5 on the Protection of Medical Data "medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor."[52] According to Article 29 Working Party's Opinion 4/2007 on the concept of personal data[53] in most of member states' legislations the personality of human beings starts with the birth and lasts until the death. "The extent to which data protection rules may apply before birth depends on the general position of national legal systems about the protection of unborn children." In case of inheritance rights, some member states consider the children that are conceived but not yet born as if they were born as far as benefits are concerned, under the condition that they are effectively born. Other member states give specific protection through particular legal provisions, also subject to the same condition. To determine whether national data protection provisions protect also information on unborn children, the general approach of the national legal system towards protection of unborn children should be considered along with the idea that the aim of data protection law is to protect individuals.

---

48 ePractice.eu, BE: Large-scale distribution of Belgian electronic ID cards to begin in September 2004, available at: http://www.epractice.eu/document/1529

49 The ID Corner, The problem with the Belgian eID card, available at: http://idcorner.org/2005/07/04/the-belgian-eid-card-calamity/

50 B. Van Alsenoy, D. De Cock, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit, 3/2008, pp. 178 – 183.

51 Belgian Data Protection Act: Law of 8 December 1992 on Privacy Protection in relation to the processing of personal data, Belgian Official Journal 18 March 1993;

52 Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997), available at: http://www1.umn.edu/humanrts/instree/coerecr97-5.html

53 Article 29 Data Protection Working Party WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Minors: In Belgium no age categories for minors are made. Everybody under 18 is considered to be minors. A minor is, in principle, the owner of all rights and duties but he can't exercise them himself and on his own. He does not have the competence to act, concerning both substantive actions and acts of procedure. He needs to be represented, but for some actions general exceptions are made (without age-limit), for example, resistance against organ transplantation or daily acts like buying tickets for a concert. Next to that there are also exceptions on actions a minor can exercise from a certain age by himself and on his own e.g.

- From the age of 16
  - Decide about gifts (art 904 Civil Code)
  - Handover acts from bailiff (art 35 Judicial Code)
- From the age of 15
  - Request for emancipation for a minor (art 479, 2 Civil Code)
- From the age of 12
  - Act in front of juvenile court

There are also some exceptions according to which a minor can act himself, but not on his own, meaning a representative will have to approve the action e.g.

- marriage
- his own adoption from the age of 12
- enter into a labour contract

Only for liability and for sanctions when the minor acts on his own, a distinction is made between minors who have and have not a "power of discernment". In the Belgian Data Protection Act no distinction is made between minors and adults. They both have the exact same rights. According to art.16 of the Convention on the Rights of the Child: "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks."[54]

Decease: The legal subjectivity ends when a person dies. His rights and duties are annulled. The moment of death is not defined in the law and therefore needs to be interpreted in a strict way. When there is the smallest sign of live, it is impossible to declare somebody legally dead. A certificate of death has to be issued. According to Article 29 Working Party's Opinion 4/2007 on the concept of personal data[55] information about deceased is not considered as personal data. The reason for such opinion is that dead individuals are not natural persons according to civil law. Such data may however get under protection for several reasons: 1. the data controller might not be in a position to ascertain if the person of whose data he is in control is still alive or not, he might process both types of data in the same way; 2. information on the deceased may be referring to living people and for that reason it needs protection; 3. it might be protected on the basis of other legal grounds e.g. right to image and honour; 4. member states are not restricted in a possibility of extending the scope of the national legislation implementing the Data Protection Directive.[56]

---

54 Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, available at: http://www.unhchr.ch/html/menu3/b/k2crc.htm

55 Article 29 Data Protection Working Party WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

56 Article 29 Data Protection Working Party WP 136, Opinion 4/2007 on the concept of personal data, adopted on 20th June, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

3.4 Poland[57]

3.4.1 National Registers Numbers

Polish citizens are obligatorily provided with a distinctive identifier- a PESEL number (General Electronic System for Citizens Evidence). PESEL numbers are used in Poland since 1979. They are mandatory for:

- all permanent residents of Poland,
- temporary residents staying in Poland for over 3 months,
- Polish citizens and foreigners who enjoy social security or health security in Poland,
- Polish citizens living abroad who apply for Polish passport.[58]

The PESEL numbers are stored in PESEL registers which contain information on:

- all names and current last names, family last name, former names and last names,
- names and family names of parents,
- date and place of birth,
- gender,
- nationality,
- number of the birth certificate and indication of the registry office that has issued the certificate,
- marital status,
- name and last name of the spouse, date of marriage, number of the marriage certificate and the indication of the registry office,
- date of termination of marriage, decision of court terminating marriage with the reference number,
- date of death of the spouse, number of death certificate, indication of the registry office issuing the certificate,
- address and place of permanent residence, former addresses and places of permanent residence, address of temporary residence,
- military rank, number of the military ID,
- number of the national ID, date of its issuance, and validity date,
- date of death, number of the death certificate and indication of the registry office issuing the certificate.[59]

The registry contains additional information on foreigners.[60]

Access to the information in the PESEL Register is restricted and the list of administration entities that have access to the Register is provided in the Law on Populations Registers and Identity Documents.

The registry is maintained on municipality level with separate registry offices responsible for issuance of birth, marriage and death certificates. The registry offices cooperate and exchange information with other registry departments within a municipality. They are obliged to inform each other about every alteration of data of residents in their municipality. The rules outlining

---

57 This section is based on the IDABC eGovernment Factsheet on Poland, January 2009, edition 11.0, available at: www.epractice.eu, and information from the website of the Ministry of Interior and Administration, http://www.mswia.gov.pl/portal/pl/381/32/

58 Art. 31a of the Law from 10 of April 1974 on Populations Registers and Identity Documents, consolidated text: O. J. 2006 Nr 139 position 993 with later changes;

59 Law from 10 of April 1974 on Populations Registers and Identity Documents, consolidated text: O. J. 2006 Nr 139 position 993 with later changes

60 Law from 10 of April 1974 on Populations Registers and Identity Documents residents' registry and IDs, consolidated text: O. J. 2006 Nr 139 position 993 with later changes

the communication between these entities are described in the Law on Populations Registers and Identity Documents.

The PESEL number has the form YYMMDDZZZXQ, where YYMMDD is the date of birth (with century encoded in month field), ZZZ is the personal identification number, X stands for gender (even for females, odd for males) and Q is a control digit.

In the past there have been several accidents regarding the attribution of PESEL numbers where different persons had been assigned with the same PESEL number. For this reason the Minister of Interior and Administration started the PESEL2[61] project for a new public registers implementation.

Apart from the PESEL Number, each citizen is provided with another identifier - The Tax Identification Number (NIP). The Number is used for entities paying taxes in Poland. It is assigned upon application which is mandatory when a person/entity starts to be a subject of fiscal duties.

It should be noted that both types of numbers have been envisaged to be used as the unique identifier in the certificate of the future eID card which is particularly relevant for the use of electronic signatures in eGovernment applications.

Moreover, both numbers: PESEL and NIP can be used as identifiers in the future for all back-office information exchanges in eGovernment applications for those who hold such numbers. The use of the national register number by the providers of applications is only allowed in specific, strictly regulated cases. Due to the fact that the national registry number is included in the signature certificate, compliance with the provisions on the use of this number is considered to be problematic. For that reason solutions have been proposed to encrypt the national registry number. Such solutions would solve possible conflicts between the validation of a certificate and the legal restrictions.

3.4.2 'PESEL2' Project

The PESEL2 project has been planned for years 2006-2008. The aim of the PESEL2 project[62] entitled 'Reconstruction and integration of state registers' is the creation of a modern State information infrastructure and improvement of the provision of eServices to Polish citizens and entrepreneurs. This strategic goal is to provide the possibility to access the information of the PESEL Register on the one hand, and build an integrated IT System as a reference register for the population registry on the other. On the operational side the project is planned to allow for the online use of the system to access the data contained in the PESEL system registers.

The PESEL2 system consists in the integration, reorganization and modernization of the existing State registers. It needs to be stressed that the information resources of the PESEL2 will only contain the data included in the current PESEL system with some changes.

The services that were planned to be implemented by 30th June 2008 should allow for online access to issue and invalidate documents, and online verification of personal and address data. The logic behind the latter service is based on sending a query regarding a very specific scope of data, then obtaining an answer whether the data is available in the PESEL2 system (YES/NO answer).

The remaining tasks, including the development of the local layer and the implementation of new information flows in the system, will be carried on under the PL.ID project planned for 2008-2013, which is a continuation of the PESEL2 Project.

---

61 Further information below.

62 More information available on: http://pesel2.mswia.gov.pl/portal/P2/14/115/O_Programie_PESEL2.html; http://www.cpi.mswia.gov.pl/portal/cpi/38/195/plID__Elektroniczny_dowod_osobisty.html;

Furthermore, legislative changes to the current Law on Populations Registers and Identity Documents will be introduced simultaneously to the implementation of PESEL2. Currently, this Law limits the possibilities of electronic access to several services for those institutions which are particularly interested in such services.

3.4.3 'PL.ID' Project[63]

The goal of this project is a development of a 'Multifunctional Personal Document' (MPD). The document which is an intelligent, PKI-ready smart card is planned to replace the traditional plastic ID card. For a successful development of identification documents a certain amount of legislative changes is required – as defined in the development strategy. The project which is the continuation of PESEL2 plans an introduction of the Polish biometric ID card for 2008-2013. The future Polish electronic ID will make use of existing identification numbers and reference databases (PESEL for individuals and REGON[64] for business).

The Act on Electronic Signatures[65] set out a deadline for the Polish Government to provide services for citizens with electronic signatures for early May 2008. It should be highlighted that the cost of an electronic Signature (at least €60) for Polish citizens are considered to be high, which results in a limited use of the few eServices requiring the use of an electronic Signature in Poland. The replacement of the national ID cards with the new ID cards preequipped with electronic Signatures together with gradual introduction of new eServices requiring an electronic Signature (e.g. tax declaration online with the new eDeclarations system) are thought to improve this situation.

3.4.4 'ePUAP' Project

The ePUAP project[66], which full name is the 'Electronic Platform of Public Administration Services' is a major task defined by the National Computerisation Plan. Its realization was scheduled for the period 2007-2010. The goal of the project is an electronic integration of all public registers as well as the creation of an integrated platform supporting a number of interactive services for citizens and businesses. The project will employ a user identification/authentication, electronic case handling and ePayments, when necessary.

A development of an integrated platform for eGovernment services was first announced in the document 'Gateway to Poland'[67] (Wrota Polski) in 2002. The ePAUP project constitutes an update of the concept presented in 'Gateway to Poland'.

The aim of ePUAP is an introduction of a full functionality of electronic service delivery at national level. The platform, created as a result of ePUAP, will be used by public bodies to ensure the availability of their services based on electronic communication channels with the use of specific basic elements (Platform services) through a single Internet point.

The next step for the ePUAP platform is to allow defining subsequent processes of services for citizens and businesses, while establishing access channels to the particular Public Administration systems and extending the set of public services provided through electronic means.

---

63 For more information see: http://www.cpi.mswia.gov.pl/portal/cpi/38/195/plID__Elektroniczny_dowod_osobisty.html;

64 National Official Business Register number assigned by the Main Statistical Office.

65 Act on Electronic Signatures, 18 September 2001, *Journal of Laws* (Dz.U.01.130.1450), available at: http://www.mgip.gov.pl/NR/rdonlyres/9C534966-8336-49C9-8087-0F4A64F14D66/18224/act_on_eSignature.pdf;

66 For more information see: http://www.cpi.mswia.gov.pl/portal/cpi/38/195/plID__Elektroniczny_dowod_osobisty.html;

67 http://www.mswia.gov.pl/portal/pl/267/3897/;

The ePUAP portal was experimentally launched by the Ministry of Interior and Administration on 14th April 2008.

3.4.5 The life cycle[68]

Birth and before: In Poland, foetus is not considered a legal subject. Legal subjectivity starts with the moment of birth. At that point every born person acquires legal capacity. The child has to be born alive. In order to consider a child as being born alive, any sign of life has to be observed. The newborn's ability to stay alive (continue living) does not matter for declaring the baby as born alive. A concept of conditional legal capacity of foetus (with condition of being born alive) is not supported by the current state of law. A foetus is not a legal subject, and does not have any legal capacity. This construction does not, however, deprive the foetus of protection. It is protected through specific regulations, mostly in the areas of family law, succession law and law of obligations.

- According to the Polish Civil Code (art. 446^1) from the moment of birth, a child can ask for reparation of damages suffered before birth;
- A child that has already been conceived at the moment of opening of the succession can be a successor (art. 927 § 2 Civil Code);
- An unborn child can be acknowledged by the father before it's being born (art. 75 of Family and Custody Code) ;
- It's possible to establish an administrator to an unborn child to protect its future rights (art. 182 Family and Custody Code)

Minors Polish Civil Law divides all the people into 3 groups based on the age:

- Age 0 -13
- Age 13-18
- age 18 – death

The difference is in attribution of legal acting power. The Polish Civil Law differentiates legal capacity – which is an ability to be a subject of legal rights and obligations, and active capacity to perform legal actions or to create such rights and obligations. The first group, aged 0-13, has a legal capacity but no active legal capacity to perform legal actions, similar to fully incapacitated persons. The second group has a legal capacity and partial active legal capacity to perform legal actions. The status of this group is the same as those who are partially incapacitated. The last group enjoys the legal capacity and the full active legal capacity to perform legal actions. Legal action performed by a person from the first group is void. However, if it is a common, normally performed action in everyday life (buying bus tickets, buying candy) it is valid unless it seriously harms the rights of the person performing it. Legal action performed by a person from the second group requires a confirmation by a legal representative of the person. Individuals with the limited capacity to create legal obligations are free to perform small legal actions of everyday life. The Data Protection Act does not make a distinction according to the age. Everybody receives the same protection.

Decease: The legal subjectivity ends when a person dies. The moment of death is not defined in the law and therefore a medical definition is used. Death is defined as 'a permanent, irreversible arrest of brain activity (cerebral death)'. In case of doubt, a commission consisting of three specialists (at least one anaesthesiologist and one neurologist or neurosurgeon) is called. A certificate of death has to be issued.

---

[68] The part is based on the Commentary to the Polish Civil Code, ed. E. Gniewek, third edition, 2008.

3.5 Sweden

3.5.1 Government

Sweden has a long history in keeping track of its inhabitants both in written as well as in automated registers. In order to make these registers more precise and to make the taxation administration more effective personal identity numbers were introduced in 1947. Sweden also makes quite heavy use of different types of identity documents and even though there are no legal obligations to have an identity card it is quite difficult to live a normal life without one. Within Sweden there are four main types of identity documents i.e. the passport, the driving license, the national identity card and SiS standard identity cards. Below we will discuss the personal number and the latter two types of identity documents. We will also discuss a new type of identity card issued by the Swedish tax authority that will be introduced during 2009 as well as the digital identity infrastructure used in e-government by some Swedish governmental agencies.

3.5.1.1 The personal identification number

The personal identification number was introduced in 1947 as a result of the 1946 reform regarding national registries where it was stated that the primary purpose of the national registry was to keep a record of the citizens for societal needs. The original personal identification number consisted of 9 numbers, but with the advent of automated data processing in the 1960s a 10th control digit was added. The number itself has the form YYMMDD-SSSC where YYMMDD is the birth date of the person with year, month and day. SSS is a three digit serial number where odd numbers are for males and even numbers for females. C is a control digit calculated using the Luhn-algorithm. Before 1990 the first two digits in the serial number where dependent on the province in which you were born with Swedish citizens born outside of Sweden having a number series of there own. This made it too easy to determine if a person was born in Sweden or was an immigrant just by examining the personal identification number. In order to remedy this, the regional division of the numbers was abandon in 1990 and was replaced by a pure serial number.

Personal numbers are used as identifiers or are, in other ways, present in most (if not all) personal registers managed by the government, medical registers and in many personal registers used in the private sector. Because of this it is quite hard to live in Sweden without one. Individuals living in Sweden are given personal identity numbers when they are entered for the first time in the national registry. However, there are people temporarily living in Sweden that do not fulfill the requirements for being entered into the national registry. These persons are instead given an identifier called a co-ordination number. This number has the same structure and function as the personal identification number however the number 60 is added to the day field in the birth date. This number is later replaced by the personal identification number if they are later entered into the national registry.
As an aside one can also mention that even legal non natural persons have a number called an organization number consisting of 6+4 digits. However, even if its structure is the same it is constructed in quite a different manner.

3.5.1.2 SiS standard identity cards

Arguably the most used identity card in Sweden is the driving license. Besides this there exists a number of different recognized identity cards that all follow the SS 61 43 14 identity card standard. The most common issuers of such a card are the banks or “Svensk Kassaservice AB” however some bigger companies also have the right to issue such cards to their

employers. In order to issue or produce a SiS standard identity card the issuer or producer has to be certified by DNV (Det Norske Veritas) according to the standard and DNVs special requirements SBC 151. Lately, "Svensk Kassaservice AB", which in essence is the only identity document issuer that anybody in Sweden can apply to, has begun to interpret the requirements for issuing an identity document in quite a strict manner. This has made it hard for non Swedish citizens to obtain a Swedish means of identification. This, in combination with the fact that many mundane tasks require a Swedish means of identification, has resulted in some foreigners who are living in Sweden having difficulties in performing specific activities ranging from renting DVD films to not being able to open bank accounts or withdraw money from already established accounts. In response to this the Swedish government has decided to give the Swedish tax authorities the right to issue identity cards based of different forms of identity assurances than the SiS standard identity cards. An example of the difference is that the new type of identity card can use non Swedish identity documents as breeder documents while the SiS standard identity cards require Swedish identity documents[69].

3.5.1.3 National Identity Card

The national identity card was introduced in Sweden in 2005. It is issued by the passport authorities to Swedish citizens and is not mandatory. The main purpose for it in Sweden currently is as an alternative to the passport traveling within the European Union. However, with a wider user base and its current capabilities one could easily envision a much wider domain of applicability specifically in the online environment. The card contains in principle the same information that is present in the Swedish passport e.g. name, surname, gender, personal identification number, height, signature and facial photograph. The card also contains two smartcard chips, one chip containing the information present on the card and a digital facial image and the other is assumed to be used in the future for storing information for eID-services. The identity card follows the ICAO standard for identity cards[70].

3.5.1.4 e-ID

Quite a number of governmental services in Sweden can nowadays be handled over the net. The array of services available range from viewing progress of a request to electronically filling out and handing in your tax form. In order to perform these e-services some form of e-ID (or digital certificate) is needed. There are three recognized Certification Authorities (CA) for this certificate: Bank-ID which is an organization run by most of the banks active in Sweden, Telia-Sonera which is a telecom operator and Nordea which is the only bank constituting its own CA. In order to obtain an e-ID you have to have a Swedish personal identification number and to be registered in the national registry. In order to get a Bank-ID certificate you also have to have an internet bank account in one of the banks within the organization. The e-ID is distributed in two different ways, either as a file that is stored on the computer or as part of a smart card. The certificate itself contains the name of the owner and (as almost always in Sweden) the personal identification number.

---

69 See" Id-kort för folkbokförda i Sverige" Betänkande av Id-kortsutredningen SOU 2007:100 and http://www.sweden.gov.se/sb/d/11669/a/123763for a more detaild discussion in swedish on these issues.

70 http://www.polisen.se/Service/Pass-och-id-kort/Fragor-kring-pass--och-id-kort/Fakta-om-ID-kort/ accessed 2009-05-12.

3.6 France

3.6.1 National Identity Card

The secured national identity card was introduced in France in 1987 to replace the paper version. It is freely available and is not mandatory however it is convenient in its size and can be used to travel to those countries who have signed the Schengen Agreement. It contains the following information pertaining to the card holder: unique identifier, name, surname, gender, date and place of birth, height and signature.

Figure 3: French Identity Card

The French government initiated a program in 2004 called ADELE (Administration ELEctronique) with the objective of modernizing public administration by electronic means, in order to simplify procedures and developing systems that are capable of securely identifying citizens. Some of the services included in this framework is a call centre service, a one-stop shop service for address change, tender submission, personalized public services portal, civil registration certificates (birth, marriage, and death certificates), and applications for funding. The collaborative platform is called ADELE 128 or is sometimes referred to as Admisource. It is destined for public bodies and is comprised of reusable software components, data warehouse and collaborative workspace.

3.6.2 National Electronic and Secured Identity Project

The INES project (Identité Nationale Electronique Sécurisée/National Electronic and Secured Identity) was presented in 2005 and it was planned to introduce an electronic identity card by 2008. Its objectives were to simplify, secure and combine the procedures related to requests for passports and national identity cards; improve their administration; deliver them in a secure manner that conforms to international demands, and, offer citizens the possibility to prove their identity on the Internet and the ability to sign electronically in order to encourage the development of electronic administration.

Reasons for initiating the project are:

- Current procedures for delivering national identity cards and passports are not sufficiently secure as the applicant may supply either false or stolen papers. The cost of this fraudulent behaviour to the French government is estimated at hundreds of millions of euro deriving, for example, from false social claims.
- Due to terrorist concerns and consequent legislation, numerous countries are enforcing the insertion of photographs and digital prints on the chips of identity cards, passports and visas.
- It is hoped to speed up the administrative process as the applicant will only have to go through one procedure for both passport and identity card applications. It is also wished that the INES process will avoid an administrative overhead related to the potential creation of separate electronic signatures by each public body.

Numerous institutions and civil rights associations raised issues about privacy, security and the use of biometric data, and the project therefore has been postponed. Amongst its provisions, it was proposed to have a central database storing biometric identifiers and a secure information process for issuing electronic identity cards.

The card will be compliant with current international standards such as the European Regulation 2252/2004 for travel documents and IASv2 for authentication and signature tools. As opposed to the paper-based identity cards, electronic ID cards will not be mandatory.

3.6.3 The National Electronic Identity Card

The card will be in the form of a bank card, with the following details written on it: name, surname, date and place of birth, gender, address, written signature, name of the prefecture that issued the card and, finally, the number of the card. The card will also contain an electronic chip that will be divided into definitive segments and secured through cryptography. The “identity” part will contain the same information that is accessible on the card as well as a biometric fingerprint and photograph data on the chip. Another part will contain “authentication of the card” that will be an anonymous mechanism which basically asks if the card is genuine. The “authenticated identity of the card holder” (also known as certified identity achieved by a secret PIN code) will allow access to online public and private services. The “electronic signature” segment will allow the signing of electronic documents destined for electronic public services. The “personal portfolio” is an option open to the card holder which permits the storing of personal complimentary information that may be used to facilitate electronic transactions such as rendering personal data exportable or to substitute other official documents like a driver’s license.

3.7 Ireland

Official identity management in Ireland is based on a unique identifier called the Personal Public Service Number (PPSN) which is assigned to Irish children when they are born and to foreigners who reside in Ireland when they register for tax or apply for social benefits. It was introduced in 1998, under that year’s Social Welfare Act, and replaced the Revenue and Social Insurance (RSI) number which was used solely for taxation and social security purposes. This act contains references to the privacy of personal data outlined in the Data Protection Act, 1988.

The Modinis Identity Management Iniative report[71] outlined that the non-mandatory nature of the PPSN (the number is only issued to those who make a social benefit claim) may exclude certain persons. Nevertheless the fact that parents usually register their children in order to receive state payments, this approach by the government can be seen as an effective means to initiate an eGovernment identity management system.

3.7.1 Public Services Broker (PSB)

The PSB is a common secure access point for electronic public services and strives to not only support customer interaction but also to provide a means for inter-agency collaboration. Once customers have registered and authenticated themselves, they are able to sign-on once to the PSB portal and access all available Government agencies through a common interface. Individuals can submit a transaction on their own behalf and also authorize agents or intermediaries to do so for them; this permits business related transactions to take place by authorized persons.

Background to PSB: In 1994 the Strategic Management Initiative (SMI) was launched with an aim to improve the delivery of public services. The resulting government report, Delivering Better Government, recommended, amongst other points, the provision of quality information and advice to customers, the integration of public services at local, regional and national levels, and to use information technology to facilitate these developments. Another report, the Integrated Social Services Strategy (ISSS), published in 1996 by an inter-departmental group, advised the use of a number as a single identifier for customers to access public services, the computerisation of the General Register Office, and the introduction of a single point of access for public service customers. The first Government Action Plan on the Information Society was produced by the Irish Government in 1999 and outlined development measures for areas such as telecommunications infrastructure, development of electronic commerce and business opportunities, legislative measures, ICTs and delivery of public services. In the same year, and as a consequence of the ISSS report, the Government established Reach to develop and deploy an infrastructure framework (Public Services Broker-PSB) for the integration and delivery of public services in Ireland. The portal went live in 2004 and the integration framework, which is based on a service oriented architecture running on a secure hardware platform, went live in 2005.[72][73]

3.7.2 Centralized Identity Management

As a result of the public services broker a new database, Public Services Database, was created and contains information which was transferred from decentralized databases. This new centralized approach is hoped to alleviate concerns over privacy issues as the PSB will be in charge of its management and the information will only be accessible through the services of the PSB. Communication through the PSB is based on an Inter-Agency Messaging Service (IAMS), which permits the exchange of information between public administrations, and on the relevant technical standards of ISO.

---

71 https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5_Identity_Management_Initiative_Report_1_IIR1.pdf accessed on 2009-05-05

72 http://www.public.ie/index.asp?docID=326 accessed on 2009-05-06

73 http://www.finance.gov.ie/documents/publications/cspvgjan05/thirdrepsgpsmd.pdf accessed on 2009-05-07

Privacy Concerns
With the express consent of the user, personal data that are used frequently can be stored centrally in order to improve the quality of the service. By building personal profiles and providing additional personal information, users can access services that are the most relevant to them. Privacy issues have been outlined under the privacy framework contained in the Social Welfare Act of 1998.[74]

Furthermore the usage of PPSNs is not permitted by the private sector or more precisely to those how are not legally mandated public entities or persons. A citizen can be assured that their personal information is maintained within a regulated structure that is transparent and the usage is made available on request as outlined in data protection legislation.

Fraud Detection
Even though a PPSN is allocated to those who apply for social benefit, there are still mechanisms in place to deal with claims based on identity and welfare fraud. The Department of Social and Family Affairs work in collaboration with the Garda (Police) National Immigration Bureau to investigate dubious applications. As a result of this activity the State made savings of approximately €300,000 per month in 2004, mainly due to the identification of false/forged documentation presented by foreign nationals[75].

Medical Card
This is issued to those who meet certain criteria such as age and level of income and is provided free of charge. Normally it is provided on a yearly basis and it covers the card holder, spouse and dependent children. With this card certain health services are free of charge such as family doctor visits, prescribed drugs, hospital services, dental care and also school transport charges, state exam fees and school books. It contains the name, address and PPSN of the cardholder as well as the doctor's name.

Public Service Cards

In June 2004, the Irish Government established an expert group to introduce a standard framework for Public Service Cards (PSC) making use of the PPSN. This card could be used for electronic identification and authentication purposes and could have a combination of functions such as a medical card, social services card.

3.7.3 Electronic Passports

In October 2006, the Passport Office in the Department of Foreign Affairs started issuing the new Irish electronic passport (ePassport). ePassports use a secure, contactless electronic chip that can store encrypted digital information. The chip holds personal details about the card holder, as well as a digital image of the person's face. The chip technology allows the information stored on an ePassport to be read by special chip readers at close range. The chip also incorporates digital signature technology to verify the authenticity of the data stored on it.

---

74 http://www.irishstatutebook.ie/1998/en/act/pub/0006/index.html accessed on 2009-05-08
75 http://www.dataprotection.ie/docs/Home/4.htm accessed on 2009-05-11

3.8 Austria

3.8.1 Bürgerkarte

In 2003 the Citizen Card "Bürgerkarte" was introduced in Austria and has subsequently been further developed. In November 2003 the Austrian Cabinet decided to employ chip-card technology to improve citizen´s access to public services and to supplement the planned health insurance card with electronic signatures. In February 2003, the first Citizen Card was introduced (Austrian Computer Society Membership Card). The current implementation is based on the signature law and the corresponding decree in the version from December 2004. In 2005-2006, several private and public-sector Citizen Card initiatives were started.[76] The "Bürgerkarte" is based on a concept that allows to design secure electronic public administration services and is therefore a card with different features for each citizen (as opposed to a passport).

Primarily the "Bürgerkarte" is a procedural signature solution that can include additional functions. For instance it can be used for the identification of the Austrian citizens in the public sector or for their identification in the social national security system, as members of chambers, officers in the public administration or students. Furthermore it can serve for payment functions (so-called Bankomaten Karte).[77]

The "Bürgerkarte" is mainly used in the public sector for identification and authentication purposes. The most common examples are the request for an attestation concerning data from the criminal record or public registration data, tax declarations and electronic signing (G2G) and receiving (G2C) of official documents.

The "Bürgerkarte" can be implemented using various technological platforms for example chip cards or USB token, such as:[78]

- National ID card
- Social security card (so called e-card)
- Students card for two regions, in which universities and subsequently students are organised
- Banking card including electronic signature
- Service card for officers in the Austrian public administration
- Signature implementations for mobile devices (smart phones and PDAs) and USB Token
- Electronic invoices (eInvoices)

In order to promote this initiative the Austrian "Bundeskanzleramt" (office of the Chancellor) provides all basic software and needed licenses free of charge.[79] As certificate authorities (CA) and registration authorities (RA) private providers such as A-Trust for chip card bound signatures or the Austrian Telekom for mobile signatures (so-called A1 signature) are used.[80]

---

76 An overview on the legislation in Austria can be found at: http://www.a-sit.at .

77 Meints/Hansen, fidis, D3.6 Study on ID Documents, Eleni Kosta; see http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf .

78 See http://www.buergerkarte.at/en .

79 See http://www.cio.gv.at/identity/ .

80 See http://www.buergerkarte.at/de/erstinfo/index.html .

Signatures and Identification

The two most important criteria that have to be fulfilled by the citizen card are signatures and identification. Just as in normal processes, citizens must identify themselves to the public authorities. They may also be asked to sign documents, such as contracts or forms.

The Austrian Signature Law (SigG) states that under certain conditions, electronic signatures fulfil the criteria for handwritten signatures. If these conditions are met, then the level of security is high enough to prevent an electronic signature from being forged (qualified signature).[81]

Like in public administration processes, also for the use of the "Bürgerkarte" a universal organisational identifier (such as social insurance number, student number, etc.) in addition to the name is needed. To ensure a more qualitative system for identifying citizens, a unique number (sourcePIN) is saved on each citizen card. This number is unique to each citizen and is derived from the unique number in the Central Register of Residents using strong encryption. This ensures that there is no confusion about the person's identity, which can otherwise happen with names that are the same.

The sourcePIN is only saved on the citizen card and is not used directly for identification purposes itself. Instead, a derivation of this number is created for each process in a way that prevents connections from being made between transactions using the sourcePIN. This derived number is referred to as a sector-specific personal identifier (ssPIN). A citizen card satisfies the security criteria required for public administration to be used for identification and signature purposes.

3.8.1.1 Data protection and Security

The "Bürgerkarte" stores personal information (identity link, such as your first name, last name, date of birth and sourcePIN), signature certificate (it contains the name and perhaps the date of birth and e-mail address), and if applicable, an electronic mandate that empowers acting on behalf of another legal entity or natural person.

Health information and other data are not saved on the citizen card. However, some citizen cards may contain additional data such as social insurance card e-card (social insurance data), Bank card (account information) or student identification card (student number). Citizen cards applications used in the citizen card environment are not able to read this additional data.

Sector specific personal identifier[82]: Based on the requirements of the Austrian data protection act for authentication purposes in the public sector the certificates for the electronic signatures are not being used to avoid linkability in cases where no signature is needed. Instead a specific personal identifier, the so called sector specific personal identifier (ssPI), is being used in addition to name and date of birth for processing and data storage purposes. The ssPI is calculated from data stored on the "Bürgerkarte". The calculation procedure for the ssPI is the following[83]:

A registration number (zentrale Melderegisterzahl, ZMR) is stored in a central database at the Citizens Register of Residents (CRR, zentrales Melderegister) for each citizen. This number is used as basic data for the calculation of a so called source PIN (sPIN). In cases where no data in the Citizens Register of Residents is available, data from the Supplementary Register (SR, Ergänzungsregister) is used as basic data.

The source PIN is only stored on the "Bürgerkarte", not in the registration office (Stammzahlenregisterbehörde, StZRBeh). In cases where this number is needed by public

81 See http://www.buergerkarte.at/en/ueberblick/index.html .

82 Meints/Hansen, fidis, D3.6 Study on ID Documents, Eleni Kosta; see http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.6.study_on_id_documents.pdf .

83 See http://www.datenschutzzentrum.de/sommerakademie/2005/somak05_kotschy.pdf .

authorities or the citizen it has to be recalculated under the supervision of the Austrian Data Protection Commission.

The public sector in Austria is divided into 26 sub-sectors and 9 sector-spanning activities; each division of a public office is assigned to one of these sectors or sector-spanning activities. In cases where a citizen starts communicating with a public office, his source PIN (sPIN) is one-way hashed with the sector identification taken from the "Bereichsabgrenzungsverordnung"[84], resulting in sector specific PIs (ssPI). The multiple ssPIs of the citizen can not be linked across the borders of these sectors. In the private sector the enterprise registration number can be used instead of the sector number to hash an ssPI.

In cases of inner-sector workflows the sector specific PI (ssPI) must be stored encrypted. In this case the ssPI can be used as a symmetric key.

The "Bürgerkarte" today is mainly used in the public sector for identification and authentication purposes. The most common examples are the request for an attestation concerning data from the criminal record or public registration data, tax declarations and electronic signing (G2G) and receiving (G2C) of official documents.

Some issues regarding the "Bürgerkarte" still remain open. In addition to the unlinkable ssPI, name and date of birth are used which are in most cases unique and thus create linkability. In case an electronic signature is needed for private or e-governmental transactions, linkability can be established via the single certificate stored on the "Bürgerkarte", as this concept does not include sector specific or pseudonymous certificates for electronic signatures.

[84] See http://www.statistik.at/web_de/frageboegen/registerzaehlung/gesetze/index.html .

Chapter 4

Identity and Education

4.1 The Netherlands

As in government there is a connection between identities and identifiers in education. In the Netherlands all pupils who engage in government funded education receive their own education number, officially called Person Bound Number (*PersoonsGebonden Nummer*, hereinafter: PGN).[85]

Since the introduction of the BSN the PGN is identical to the BSN.[86]

The aim of the PGN is to allow closer monitoring of pupils. The government collects information on the compliance with legal obligations to attend school up to a certain (nationally determined) age and drop-outs. The number is also used in communication between educational institutions, the city administrations and the central government.[87]

The PGN is connected to the individual pupil. However, in the Netherlands there is a separate communication system for institutions for higher education, facilitated by the SURFfederation[88]. "The SURFnet Federation will ensure that users can prove their identity by making use of data which this organisation (an educational institution), known as the Identity Provider (IdP), issues and manages for this purpose. The point of departure is the privacy of the user. It is therefore the task of the Identity Provider to determine the user's identity, and to issue it to the federation, in combination with a number of user characteristics, where appropriate.

In turn, the SURFnet Federation ensures that information and service providers trust the information regarding this identity. This prevents users having to remember multiple login names and access codes, and prevents the organisation having to maintain a large number of technical connections to information and service providers."[89]

---

85 See: http://www.postbus51.nl/nl/home/themas/rechtspraak-en-veiligheid/identificatie/burgerservicenummer-bsn/wat-is-het-onderwijsnummer-en-hoe-kom-ik-eraan.html (last visited: December 2008).

86 See: http://www.postbus51.nl/index.cfm/t/Wat_is_de_relatie_tussen_het_onderwijsnummer_en_het_burgerservicenummer__BSN.html(last visited: December 2008).

87 See: http://www.postbus51.nl/index.cfm/t/Wat_is_het_onderwijsnummer_en_hoe_kom_ik_eraan (last visited: December 2008).

88 See: http://federatie.surfnet.nl (last visited: December 2008).

89 See: http://federatie.surfnet.nl/cms/content/view/16/1/lang,en/ (last visited: December 2008).

Within the SURFnet Federation authentication and authorisation data are exchanged based on the SAML (Security Assertion Markup Language) standard. [90]

The SURFnet Federation is an identity provider based on A-Select technology. Organisations (institutions and other service providers like publishers) can all become members individually.[91]

Depending on the purpose of the connection specific attributes are provided to a service provider. The table of all data and attributes concerning one person as provided to the SURFnet service provider itself looks a follows:

Subject: **s606336**

Name	Value
urn:mace:dir:attribute-def:uid	s606336
urn:mace:dir:attribute-def:mail	A.P.C.Roosendaal@uvt.nl
urn:mace:dir:attribute-def:eduPersonEntitlement	urn:mace:dir:entitlement:common-lib-terms

Table 4: Attributes and values, source: https://wayf.surfnet.nl/federate/attributes.

The subject s606336 refers to a student with number 606336. Depending on the service provider all of these data, only part of them are provided.

For instance, Elsevier ScienceDirect receives the following information concerning the same individual when entering the ScienceDirect site for journal article download:

Subject: **D31A16026DD5E0A2B3C7A2A759E06132**

Name	Value
urn:mace:dir:attribute-def:eduPersonEntitlement	urn:mace:dir:entitlement:common-lib-terms

Table 5: Attributes and values provided to ScienceDirect, source: https://wayf.surfnet.nl/federate/attributes.

Here, the subject is no longer identical to the student number and only the entitlement is provided.

4.1.1.1 The IB-groep[92]

The *Informatie Beheer Groep* (IB-groep) is the Dutch government agency responsible for student grants administration and management of related student and educational information. Until the early 2000s, the agency was heavily criticised because of slow responses and bureaucratic delays. A strategic reorganisation with a focus on Internet-based delivery of services had to solve these problems.

The IB-groep developed a unique authentication concept using mobile phones and SMS; this channel was selected specifically because students often misplace electronic tokens or other e-solutions, but generally do not lose their mobile phones. The SMS e-authentication concept was offered to DigiD, and it was adopted as the Dutch middle-level e-authentication system.

---

90 See: http://federatie.surfnet.nl/cms/content/view/96/57/lang,en/ (last visited: December 2008).

91 Valkenburg, Peter/Jurg, Peter (2007). *Identity Management; omgaan met elektronische identiteiten*, The Hague: ICT Bibliotheek, p. 83.

92 Compare: OECD (2007). OECD e-Government Studies Netherlands, p. 267-269.

After logging in with DigiD and SMS e-authentication, students have access to their personal online portal (*Mijn IB-groep*) for student loans. The portal also grants access to different processes pertaining to school and higher education affairs and information. Prospective students are offered options to search databases, find courses, and apply for some programmes.

The IB-groep contains all the information on education and loans of students in one central system and maintains interactions with educational institutions concerning starting and ending or finishing studies.

4.2 Germany

In Germany the education system is in the authority of the federal states. There is only limited interoperability and similarity between day-care centres, schools and universities in different federal states.

As soon as the child reaches the age where school attendance is compulsory (usually between the ages of 5 and 7, depending on the federal state and the child's birth date), the data from the Melderegister are transferred to the school that the child is likely to apply for (based on geographical location). If parents decide to apply for another school they have to show a written statement from the other school that the child is going to visit this school. The trigger for starting this process is the Melderegister, which identifies the eligible children on the basis of their age.

As soon as parents enrol their children at a certain school or day-care centre, this institution requires the parents to disclose certain personal data of themselves and of their child. These data often refer to other areas not specific to education (like medical data in the case of emergency or the parents' professions as institutions like to know the background of the children).

Usually there is no direct electronic data exchange between different schools and universities. Instead paper based certificates are used to enrol at another institution. Within the federal states often standard forms are used, but there are differences between the states for the various certificates.

However, in 2006/2007 an initiative of the "Standing Conference of the Ministers of Education and Cultural Affairs of the Länder in the Federal Republic of Germany (KMK)" received public attention in Germany. For statistical purposes the KMK seeks to introduce an education database in the Länder and possibly also a national education database.[93][94] Germany is reporting educational statistical data to the OECD, UNESCO and EUROSTAT. The introduction of a "core data set" ("Kerndatensatz für schulstatistische Individualdaten der Länder" - KDS) for each student was already decided in 2003. The goal is to collect data about (currently high school and vocational school) students' "education history" (Bildungsverlauf) and to allow linking data from different years for one student even if s/he moves to another Land or changes school. In order to allow linking data sets from different years a unique identifier for each student is assigned.[95] The KMK states that pseudonymity will be ensured by means of using "one-way encryption" (Einwegverschlüsselung) when creating the data sets. The following data items are contained in the KDS:

- attribute data set (Merkmalssatz) about reporting school
- attribute data set of class and courses at reporting school
- attribute data set of teaching unit at reporting school
- attribute data set of students of reporting school
- attribute data set of high-school graduate and high-school drop-outs

---

93 http://www.kmk.org/statistik/schule/statistische-veroeffentlichungen/faqs-frequently-asked-questions-zum-kerndatensatz-und-zur-datengewinnungsstrategie.html

94 http://www.fdpfraktionberlin.de/dokumente/0313bildungsregistersen.pdf

95 http://www.kmk.org/fileadmin/pdf/Statistik/FAQ_Januar09.pdf

- attribute data set of teachers at reporting school
- attribute data set of teacher fluctuation at reporting school
- optional data

The attribute data set of students contains information about the students which have a high granularity:

- year of reporting
- location of school: land (as in Länder)
- school ID number
- type of school
- level of education
- class ID
- student ID (now called data base pointer - Datensatz-Nummer)
- grade
- gender
- month and year of birth
- year of enrolment
- country of birth
- if country of birth not Germany: year of immigration
- nationality
- if German is predominantly NOT used in family: which language is spoken in family
- school background: what type of school attended in previous year
- school background: what grade attended in previous year
- kind of repetition
- educational background: school qualification
- foreign languages (in order of enrolment)
- focus of support (Förderschwerpunkt)
- participation in all-day education
- place of residence.

The Data Protection Commissioners as well as privacy activists have criticised the concepts because they fear that the “Schüler-ID” may be linked with other data.[96]

4.3 Belgium

4.3.1 EDISON[97]

EDISON (Electronic Document Interchange between Schools and the "*Onderwijsdepartement*" (Department of Education)) is a project of the Belgian Department Of Education for the Dutch speaking Community. It started in September 1991, when all 1100 secondary schools were invited to send in the statistical data collected annually in a file format on diskette.

The next step was to prepare EDI for all documents being interchanged between the Education administration and the schools.

Data had to be collected with a valid digital signature because the information is used to process the payment of teachers’ salaries and to calculate school subsidies.

---

96 http://schueler-id.de/ (last visited: December 2008) and http://www.datenschutz.de/privo/feature/detail/?featid=6 (last visited: December 2008).

97 This part is based on information from: http://www.ond.vlaanderen.be/English/, http://www.ond.vlaanderen.be/edison/Algemeen/Info/edison_EN.htm

In 2005 all schools were be invited to join and work with this new state-of-the-art e-government webservice.

In the school year of 2007/2008 the system has been upgraded into WebEDISON. The main difference between EDISON and WebEDISON is that in the new version there is no need to install software on a computer to transfer the data. In the current version data is transferred via Internet. The access to the WebEDISON is now based on the eID or federal token. The decision on who will have access to the system is made by the principal of each school.[98]

4.4 Poland[99]

Electronic student cards (ELS - Elektroniczna Legitymacja Studencka) were introduced by the Decree of the Minister of Schooling and Higher Education about documentation of the course of studies[100] from November 2, 2006 that came into force on the 1st of January 2007. The Decree provided an annex with an exact description of electronic student cards.

According to the annex, student cards contain a picture of the student, the full name of the student, name of issuing school, issue and expiry date, national identification number (PESEL), address, student registration number, and a bar code. The card contains also a chip with the same information. The information on the chip is signed with a qualified electronic signature of the school issuing the card.

The card is validated with a hologram sticker for each academic year.

Additionally, electronic student cards can serve as a periodic ticket for public transportation, parking ticket, library card and entry card into students' dormitories. In future it will contain also student records.
Personal files of students, documenting their course of studies and all administrative decisions concerning students are stored in the school for 50 years.

98 http://www.ond.vlaanderen.be/edison/webedison/voorbereiding/default.asp

99 This section is based on articles from www.vagla.pl, and information from: http://www.mcp.poznan.pl/;

100 Decree of the Minister of Schooling and Higher Education about documentation of the course of studies from November 2, 2006, DzU nr 224, poz. 1634, available at: http://www.bip.nauka.gov.pl/_gAllery/15/58/1558/20061102_rozporzadzenie_dokumentacja.pdf

Chapter 5

Identity and Health Care

5.1 The Netherlands

5.1.1 The life cycle

Pre-Birth and Birth: In the Netherlands the foetus is legally protected but not considered to be a legal subject yet. This changes as soon as the child is born. From that moment on, the child becomes bearer of rights and becomes part of the legal community equal to all other humans. After birth, the human being obtains the right to have a name[101] and the child gets a father[102]. The only requirement is that the child is born alive.[103] In accordance with Article 1:19 DCC the birth has to be registered. From an identity perspective this means that a foetus is known at some medical instances, like for instance a family doctor, a midwife, and possibly a hospital. This implies knowledge on the identity of the mother, father, other family members, and eventually heritable diseases. The set of data available already forms an identity. From the birth on, this identity will be registered together with name, address and information on the date and time of birth; now the child has legal subjectivity. In particular, medical instances will keep a record containing information on the delivery and data on the pre-natal and post-natal tests of the baby. The parents of a child have to obtain a health insurance for their child. The child receives its own insurance policy which contains a personal reference number, as well as the Citizen Service Number (Burger Service Nummer, hereinafter: BSN) of the child, which is issued by the government.

Minors[104] In the Dutch health care system, minors are divided into three categories, namely minors from 0-12 years, from 12-16 years, and from 16-18 years. In practice, adulthood in the context of health care is reached at 16. This is because from that age on the minor is considered to be capable of closing an agreement regarding his treatment and performing all legal acts directly related to that agreement.[105] Until the age of 12, treatments concerning the child are agreed upon by its parents or other legal representatives. However, the minor himself becomes the contracting

101 Article 1:4 Dutch Civil Code (*Burgerlijk Wetboek*), hereinafter: DCC.

102 Article 1:199 DCC.

103 Compare: Leenen, Henk/Gevers, Sjef/Legemaate, Johan (2007). *Handboek Gezondheidsrecht; Deel 1 Rechten van mensen in de gezondheidszorg*, Bohn Stafleu van Loghum: Houten, p. 137.

104 Based on: Leenen, Henk/Gevers, Sjef/ Legemaate, Johan (2007). *Handboek Gezondheidsrecht; Deel 1 Rechten van mensen in de gezondheidszorg*, Bohn Stafleu van Loghum: Houten, p. 169-171.

105 Article 7:447 DCC.

party. If a child is between 12 and 16 years old, the minor can enter into contracts concerning medical treatment. However, the permission of the parents or other legal representatives is required.

Decease When someone dies legal subjectivity ends. The dead body, however, is protected. Before burying or cremating the body there needs to be a declaration of death.

5.1.1.1 Registers and identities

During the life of individuals all kinds of medical records are made up. In order to explain how this roughly works in the Netherlands it may be useful to indicate that health care itself is divided into categories. In general, there are two main categories, namely public health care and somatic health care. Public health care concerns vaccinations and medical examinations of the population. Somatic health care includes all other aspects, such as physical and mental care.

Basically, all information concerning an individual is documented in dossiers. Each dossier can be seen as a partial identity of the individual concerning one or more specific aspects of his health. There are many situations where medical records are exchanged, partly or as a whole, between different institutions. This exchange is done by the institutions.

Since June 1st 2008, the BSN is used in health care as a result of the Act on the use of BSN in healthcare[106] entering into force. This means that since then data are being exchanged based on the BSN and identification. The data that are being exchanged are personal data, medical data, and data about declarations.[107]

Based on Article 35 of the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*, hereinafter: WBP) patients have the right to know which health care providers, organisations indicating health risks, and health insurance organisations have consulted their personal details. The patient can obtain insight into who has:

- asked for his BSN
- verified his BSN
- asked for personal data
- verified the validity (is it in circulation) of his identity document

These requests may only concern personal details, not medical data.[108]

With the use of the BSN in healthcare, all medical records are directly connected to one unique identifier representing an individual. The use of the BSN is seen as a necessary requirement for the introduction of the Electronic Patient Record (*Elektronisch Patient Dossier*, hereinafter: EPD). With the EPD health care providers can gain access to medical records of colleagues. This takes place via a gateway known as the National Switch Point (*Landelijk Schakelpunt*, hereinafter: LSP) which authenticates the access to specific (parts of) files.

With the introduction of the BSN in health care, all identities of an individual related to health care can be referred to with one number. Before the introduction, all institutions used their own specific number to identify a patient.

There is a right to keep medical records for 15 years. Usually, this term restarts whenever something is added or changed in the record. This means that decease is possibly the last change

106 Wet gebruik burgerservicenummer in de zorg (Wbsn-z).

107 See: http://www.infoepd.nl/informatiepunt_com/zorgconsument_bsn_in_de_zorg.php (last visited: December 2008).

108 See: http://www.infoepd.nl/ufc/file2/informatiepunt_sites/marjan/75df15af62d8bcd0aaeabccf3fcafc5a/pu/De_wet_BSN_Z_op_hoofdlijnen.pdf (last visited: December 2008).

in the records in case a doctor or other health care provider is involved. Thus, the records remain stored for 15 years after the death of an individual. There is also an option to ask for destruction of the records.

5.2 Germany

So far each insurance company belonging to the German compulsory health insurance fund gave health insurance numbers to their members separately. The cards only contain administration data like the insurance company, the name, date of birth, address and insurance status of the member as well as an expiration date. Whenever an individual changes insurer before the expiration date he should no longer use the card, but there is no guarantee that people actually refrain from using the cards. Individuals and their right for treatment are the only attributes indicated on the card and this therefore allows the identification of children who do not hold a personal ID card.

So far medical data about the individual who actually use the card to get medical treatment are not stored on the card but are kept local at the medical practices (sometimes still only in written form but more often also electronically). Communication between different medical practices is still done through the patient itself who gets a letter or referral to present at another medical practice.

With the introduction of the new electronic health insurance card, the cards should also contain electronic pictures of the card holder. The insured will also get new health insurance numbers to be provided by a new central authority ("Vertrauensstelle Krankenversichertennummer")[109] instead of by the insurance companies themselves. These numbers were already created from the pension insurance number by cryptographic means in March 2006 for internal use but the members will not get them before they get the new electronic health insurance cards that are already overdue. The new numbers consist of 20 numbers and contain a changeable[110] and an unchangeable part that is valid for a person's whole lifetime (cp. Table 6):

Digit	Content / Meaning	Example
1-10	unchangeable part (linked to the member)	1234567890
11-19	changeable part (linked to the insurance company)	123456789
20	error checking number	1

Table 6: New health insurance number in Germany.

The new electronic health insurance card will no longer only contain administration data but also medical data cf. § 291a SGB V:

- a function to transfer prescriptions
- a credential on the right to get medical treatment within the EU
- the accounting information vf. to treatment by SHI-authorized physicians

The electronic health insurance card also has to be able to contain cf. §291a Abs. 3 SGB V:

- medical data for treatment in the case of emergency
- medical certificates containing clinical findings and treatments ("elektronischer Arztbrief")

[109] https://kvnummer.gkvnet.de/ (last visited: December 2008).

[110] The changeable part contains numbers from the insurance and changes with every change of the insurance company.

- data for medicinal safety
- medical data about clinical findings, injections, allergies, blood group etc. (“elektronische Patientenakte”)
- data offered by the member itself (e.g., living will)
- data about the benefits the member received cf. § 305 SGB V

5.3 Belgium

There is no general health database in Belgium. Most people have a general practitioner who collects the data throughout the life of a patient but it is not obligatory and a person can always change his general practitioner. The general practitioner shares the data with a specialist upon a consultation, but only if it’s done through the general practitioner. If a patient decides to go to the specialist ‘on his own’, there is no information interchange, unless the patient gives his consents.

There is a possibility to have the health data stored in a Centralized Medical Database which is done by the general practitioner. It is only upon request and the cost has to be covered by the patient, who later is reimbursed by his health insurance company (Ziekenfonds, Mutualitates). In that case all medical information is sent to the general practitioner.

Medical data has to be stored for 30 years.

5.3.1 SIS Card

A SIS Card is issued to every person who is entitled to health insurance in Belgium. The card is protected and is issued by the health insurance funds. No medical data is stored on the SIS card.

When the child is born, it’s issued with a so-called "social insurance identity certificate". The parents are provided with the paper document in anticipation of a genuine SIS card. It may take about 1 to 2 months before receiving an SIS card for a child. Up to the age of 25, a person can remain insured as a dependent on the parents' file. However, as soon as he begins working, receives unemployment benefit or becomes older than 25, he will have to register as policy holder on his own file.

The SIS card contains two types of information: visible and invisible. The former group consist in a national registration number - a personal code that is issued when a person arrives in the country or when a child is born. The combination of letters is specific to each individual. Apart from that the card contains: last name, first name, middle name, date of birth and a symbol to show whether the card owner is male or female. Moreover, there is an additional 10 figure number which forms the SIS card number. This number is featured in a national list providing an overview of the SIS cards that have been issued. The chip included in the SIS card includes the following information: national registration number; last name, first name, date of birth, SIS card number, name of the health insurance fund, and information about the holder’s rights to be reimbursed for the costs of medical treatment.

Health professionals use a special piece of equipment to read information on a SIS card. The equipment may only be used by specific individuals and establishments (such as the pharmacist, a health insurance fund, hospital).

5.3.2 E-health platform[111]

The federal e-Health platform's, launched in 2008, goal is to support and facilitate electronic data exchange and service provisioning among all actors of the health care sector.

Its tasks are:

- specifying a basic architecture, and the technical norms and standards to be adhered to by participants;
- providing a platform for secure data exchange, and the related basic services;
- managing and co-ordinating ICT-related aspects of data exchange from and to electronic health records, as well as electronic medical prescriptions;
- acting as an independent third party for the encoding and anonymization of health data for scientific research purposes or policy support.

In order to ensure a secure data exchange, the e-Health platform will provide: an integrated system for user and access management, timestamping, end-to-end encryption, and a secured electronic mailbox. These are considered to be the basic services of the platform. Additionally, it will provide value-added services like: consultation of the insurance status of patients, transmission of electronic invoices from nurses to health insurance funds, cancer registration services, etc. This list keeps being updated.

The e-Health platform does not store any medical data relating to patients, as its purpose is to enable the exchange of such data among authorized actors. In the future, the e-Health is planned to manage its own reference directory, similar to that of the CBSS (indicating which data is available where, which entities have a 'relationship of care' with a particular patient, etc).

5.4 Poland

There is no central medical database in Poland. Most people have their general practitioner, so called 'first contact doctor' but this is not obliged and the doctor can change throughout life. General practitioners can refer a patient for a consultation to a specialist but such consultation can be done on 'one's own' and in such case there is no communication between the GP and the specialist.

Access to medical records is regulated through the administrative regulation on Medical Records. Medical records contain a written statement of the patient indicating a person authorised to obtain access to the patient's medical record in case of his death. The statement can also prohibit any access to a patient's medical records after his death.

Medical records are stored for 20 years from the end of the year when the last entry was made.

5.4.1 eHealth card project[112]

The National Health Fund (NFZ) is currently working on implementation of the national eRegister of medical services (RUM). By the end of 2009 all Poles will be in possession of e-RUM cards. The national eCard follows the example of the Silesian Province, where electronic health cards have been used by 5 million patients since 2001.

---

111 This section is based on information obtained from the e-Health website (https://www.ehealth.fgov.be/) and the Law of 21 August 2008 for the creation and organization of the e-Health platform (Belgian Official Journal, 13 October 2008).

112 The part is based on the IDABC eGovernment Factsheet on Poland, January 2009, edition 11.0, available at: www.epractice.eu

This electronic insurance card will allow patients identification, transactions authorization, and confirmation of the scope and period of eligibility. It's worth noting that the e-RUM card will not store any medical or case history data but it will provide access to medical data stored centrally in electronic form. An individual will be identified in the card through the PESEL number. The cards will be secured with a PIN code and biometric data in the future. The introduction of e-RUM cards is expected to streamline the flow of patient information between healthcare institutions while reducing costs (approximately 10 % savings of all the annual healthcare expenditure).

5.5 France

5.5.1 Health Insurance Card

The health card (Carte Vitale) is an electronic health insurance card that was first distributed in 1998 and is issued to all individuals over 16 years of age who are entitled to be reimbursed by the social security. It possesses 4 kilobits of memory respecting the ISO 7816 standard and contains administrative information of the cardholder, spouse and children, for example their social security numbers, a code composed of the applicable health plan and the assigned local center; it does not contain medical information.

Figure 4: Carte Vitale 1

The next generation of the health card (Carte Vitale 2: figure 5) is now in place with an electronic chip of 32 Kb and the information contained on it is encrypted. The encryption uses IAS (Identification, Authentication and Signature) software and SmartMX technology developed by NXP Semiconductors. It is made available to new applicants and as a replacement to the first card in cases of loss and deterioration. The new card has added functionalities allowing it to combat against fraudulent use and also to improve the quality of healthcare.

In the latter context it could include emergency information such as a contact person or details of the doctor's patient, and information on allergies or regular treatment. With respect to the abuse of the health card evident in the previous version, the new model guarantees that the card holder is authenticated as such. It also contains a photo on the card and a digital version on the electronic chip.

Figure 5: Carte Vitale 2

Chapter 6

Identity and Employment

6.1 Employed

Once an individual is employed, several actors collect and use information about him. First of all, there is the employer who collects information even before a contract is signed, such as a Curriculum Vitae and personal notes from an interview. Then, there is of course the contract itself, which contains general data (name, address, date of birth, etc.) as well as specific data on the type of employment, salary, and conditions for the employment.

Employment data in Europe are shared with other parties, such as tax authorities and social security services and pension funds.

Also additional information might be needed and stored. Examples are:

- **The Netherlands:** If an employee becomes a member of a union this adds another attribute to his identity.
- **Germany:** Data on the membership in a religious group is collected because of the Kirchensteuergesetz and Kirchensteuerordnungen that regulates what percentage of income tax is collected directly from the income as church tax (Kirchensteuer). This does not only concern the person employed but also his spouse because if he belongs to another church the church tax is divided between the churches.

During their lifetime, most people switch jobs occasionally. Each time a new job is accepted, a new dossier is made up. Sometimes, recommendations or references of former employers and clients are attached to the job application. In these cases, the connection between the new job and former affiliations is made by the applicant. However, it is also possible that an employer gathers data about job applicants concerning their past performances. Sometimes this is done by asking former employers directly, sometimes the Internet is of help. 'Googling' applicants or searching for their Facebook or LinkedIn profile pages has become a common practice for recruiters.

Not only employers collect and merge data. Also (governmental) institutions do so in order to be able to check tax filings and pension funds, and for statistic purposes.

6.2 Unemployed

In the European countries we studied there is also data collected about unemployed people to help them find a new job and/or pay unemployment compensation.

6.2.1 The Netherlands

As of January 1st 2008, the Dutch government has implemented the Digital Client Dossier (Digitaal Klantdossier, DKD). This dossier contains all the information known about an unemployed individual at different institutions concerning employment and social security services. The information is digitally available to these institutions and prevents individuals from having to provide the same information several times. "The Digital Client Dossier (DKD) is like an 'electronic dossier'. Or to be more precise, a specialized database designed to collate information about the unemployed from the different local authorities and social services involved in getting someone back to work."[113]

Since January 3rd, citizens can consult their own digital data in the dossier.[114] Individuals have access to the dossier via the Internet, whereas institutions have access via Suwinet-Inkijk[115], which is an application that gives a contextualized overview of the available data in a protected environment that uses authorisation.[116]

The employers of the relevant institutions only have access to information that is relevant for their work, so they will not see all information at once. If an individual wants to see the available information concerning him, he can do this via the Internet using his DigiD login code to get access.

6.2.2 Germany

When becoming unemployed in Germany, the Bundesagentur für Arbeit is responsible for job-seeking and paying unemployment compensation.

For job seeking the citizen has to fill in a detailed profile of his competences and experiences that can be used by the Bundesagentur für Arbeit to match the profile to job offers and also for companies themselves to look for an appropriate job candidate.

For unemployment compensation personal and especially financial information of the unemployed and possibly also his spouse is needed by the Bundesagentur für Arbeit to calculate the correct rate of unemployment compensation and to prevent misuse.

---

113 See: http://dkd.nl/the_digital_client_dossier_english_version/ (last visited: December 2008).

114 See: http://dkd.nl/home/nieuwsarchief/nieuwsitems/archive/2008/01/?tx_ttnews%5Btt_news%5D=13&cHash=b8c9509486 (last visited: December 2008).

115 See: http://dkd.nl/digitaal_klantdossier_in_het_kort/ (last visited: December 2008).

116 See: http://dkd.nl/het_dkd_gebruiken_informatie_voor_klanten/hoe_zit_het_met_de_privacy_en_beveiliging/ (last visited: December 2008).

6.2.3 Belgium

After graduating most Belgians register themselves in one of the Public Employment and vocational training services: VDAB[117] for Flanders, Le FOREM[118] for Wallonia, ACTIRIS[119] for Brussels-Capital region or ADG[120] in the German-speaking community.

On the social level the main concern of these institutions is to put employers and jobseekers in touch with each other. In order to do so, they register unemployed and collect their CVs in a database where they can be consulted by the employers. It's worth noting that in case a person does not have a social security number, he cannot publish his CV by himself and needs the assistance of a counsellor to post the CV in the database.

In order to apply for unemployment benefits, a person needs to be registered appropriately to the area where he lives.

Moreover, these institutions provide services like job guidance, integration guidance, training courses and career guidance.

The functioning of these institutions is based mainly on the social security numbers.

6.2.4 Poland

In order to receive the unemployment benefits and maintain social security while unemployed the registration to ZUS (Social Insurance Institution) is necessary. Individual is identified through the PESEL number explained in more detail in section 3.4.1.[121]

There is also the e-PULS project, a service offered by the Ministry of Labour and Social Policy, consisting of an online list of job offers uploaded by local branches of the Employment Office. It's possible to view the offers with description without registration.

6.3 Pension Insurance Fund

The German pension insurance fund number is issued by one of the federal German pension fund insurance agencies. The number is used to organise their policyholder's cases. Further usage by other social insurance agencies, like health or nursing care insurance, as well as authorities, courts, employers, etc is legally restricted.

In contrast to former procedures, today every new born child receives his personal insurance number (cf. § 290 Section 1 p. 4 SGB V). However, a social insurance card is still not issued before the first gainful employment.

The pension insurance fund number of a person consists of twelve alphanumerical digits as described in Table 7.

---

117 Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding, http://vdab.be/;

118 Le service public wallon de l'emploi et de la formation : http://www.leforem.be/index.html;

119 Brusselse Gewestelijke Dienst voor Arbeidsbemiddeling/ l'Office Régional Bruxellois de l'Emploi: http://www.actiris.be/;

120 Arbeitsamt der Deutschsprachigen Gemeinschaft (ADG): http://www.dglive.be/

121 See section 3.4.1 on National Registers Numbers, page 31.

Digit	Content / Meaning	Example
1-2	Area of the insurance agency that issued the number	26
3-4	The assured's day of birth	03
5-6	The assured's month of birth	08
7-8	The assured's year of birth	69
9	Initial letter of the assured's maiden name	M
10-11	Serial number (00-49 = male, 50-99 = female)	03
12	check digit	5

Table 7: Structure of the German pension insurance fund number.

The relevant legal regulations can be found in § 147 section 2 Sozialgesetzbuch (SGB) VI.

The pension insurance fund number cannot be used for health insurance purposes to ensure a citizen's privacy (cf. § 290 Abs. 1 S. 4 Sozialgesetzbuch (SGB) V). The introduction of a uniform social insurance number is banned to prevent this number becoming a unique personal identification number.

However, since the new legislative regulations from 2003 the pension insurance fund number is used to generate the health insurance number by means of a cryptographic algorithm that guarantees unlinkability between both numbers.

From the legal point of view, linkability is prevented by restricting the usage of each number to the particular area of responsibility.

Chapter 7

Identity and social networks

7.1 Data linking different persons

7.1.1 Medical data

There are several scenarios possible where data are at stake that (can) belong to more than one person. A first scenario concerns medical data about an individual. At first glance, there is only one individual involved then. However, in the case that these data concern data on hereditary diseases, also family members can be involved. When taking into account that there might be something like a 'right not to know' for people when they appear to have a higher chance to get a specific disease, some questions arise. To start with, there has to be clarity on the storage of the data and who has access to these data. A particular question concerns connecting data from family members in order to include the risk to the health records of the family members for whom the risk has not yet been recognized directly. Also, when the data only get connected to the specific individual, the possibility of access to the data by family members needs to be taken into account.

Similar access questions arise when someone is deceased. Do family members have access to the data of their deceased family member? And if the health records contain data concerning hereditary diseases which thus also affects the other family members, does this imply specific duties for the health care providers to keep these data shielded? Probably, confronting people with these data is not the most favourable option. However, there can be an exception for emergency cases.

A final question is whether and when data should be deleted and how. Probably, anonymisation is sufficient, because there is always a chance and an interest to keep data preserved for later investigations, such as historical or statistical purposes. However, there is a notion in medical research that if data from living people is used in research on treatable but grave diseases like e.g. cancer it would be unethical not to be able to de-anonymize the data and offer treatment to a participant that is found to have the disease but not yet to know of it. Or if other complications are found during research. This complicates the anonymisation problem with medical data for research.

Requirements can be legal, like regulations on who is allowed to do what with medical (hereditary) data, or technical, like providing (un)linkability of data and individuals, and providing a special access treatment in emergency cases.

7.1.2 Genetic data in biobanks

Genetic data can belong to a single identity and the data do not change or evolve over time. Genetic data can probably be hidden, but not changed. (However, technological methods to adapt genetic structures are currently being developed)

Even though genetic data are very individually bound, connections between people can be revealed by the data. This also becomes clear from the fact that genetic data are commonly used for solving parenthood issues, such as father-son/daughter relationships.

7.2 Data about other persons

In this section, we discuss the aspects of life-long privacy in the new technologies of the Web 2.0.

The starting ideas for the concept were the following:

- For social networks, the individuals that have less influence on how their privacy is affected are minors and elderly: minors can have an immature view on their privacy, while elderly may lack the technical abilities to actually control their privacy.
- Identity generation fuzziness: it may not be clear at which point in time an ‘identity’ is formed: when an individual leaves traces on social networking sites, an identity might be constructed by just retrieving (and linking) all traces. Using advanced data mining technology, an identity of an individual might be constructible without the subject knowing.
- Identity control: identifying/reputation information can be distributed by others without the subject’s consent/knowledge. This is related to the previous point, but in this case, actual information about an individual is generated or distributed. This might include background personae in pictures. Should an individual be able to get control over it?

7.2.1 Children

Parents post pictures of their kids on the web. Some even post medical data on them, or make an extensive website for the kid. Direct marketing companies may also use social network sites to harvest data on the kids and to send targeted commercial messages to the parents. The problem is that at the time these data are distributed, the parent is the legal representative of the child, and therefore also exercises the rights on his/her private data. Some matters that arise:

- As these babies grow old and turn 18, they should be able (legal obligation) to get control over these data. This is because the parent stops being the legal representative of the person, and should get consent of his son/daughter for every piece of content on the parent's SNS profile, that has the son/daughter as a data subject.
- If someone's parents post data that are incorrect and may be harmful (showing/indicating disease), later on, he is allowed to ask for deletion/correction of these data. Moreover, the

parent may face legal consequences in very harmful cases of privacy breach, where they did not properly protect the privacy of the kids they were representing at the time.

7.2.2 Identity formation

Given the vast amount of data in social network sites we imagine that it's possible –or at least will be possible– to scan the data for the existence of 'hidden' identities, i.e. identities of people that do not have a social network account. A similar question can be formulated for the people with accounts: can their profile in their SNS account be extended/enriched by advanced data mining of the data in the network? Simple examples include the scanning of images for faces and known backgrounds and combining it with EXIF data in the picture file (time, date, location …). The technology for doing this is the subject of current research, and some implementations already exist as shown by Picasa[122]. A similar reasoning can be performed for traffic analysis combined with data analysis: postings to one's profile have (actor, time, and location) characteristics and their frequency also bears a meaning. Patterns of postings can be investigated, and even linguistic analysis can be conducted to extract information and shrink the anonymity set of the poster. It's not clear to which extent these techniques are legally allowed, and one possible reason for this is that it may be very hard to determine when a collection of data actually becomes identifying information.

Protection mechanisms against this include more fine-grained access control to profiles, anonymous authentication, and making data unreadable for SNS operators.

7.2.3 Control

Public facts and pictures about individuals can be posted on SNSs without the subject knowing it. Cyberbullying appears to be already common in youngsters' worlds[123] , and even in professional circles, gossiping occurs[124]. If no suitable mechanisms exist to deter wrong or harmful information, a person's reputation might be harmed for an extensive period in time. This even applies to information, posted by the individual him/herself: police computer crime units have seen a rise of parents asking to 'remove' information from the Internet, that their kids have posted themselves. Having the ability to remove or at least add contextual information to these kinds of data might be very useful.

7.3 Data about deceased persons

People's data on the Internet might still be accessible after they die. In that case, does the SNS provider have the right to exploit the data in their profile? Apparently, in some cases, they have that right, but there can also be a (moral) duty to make the profile data inaccessible. This becomes more important if the SNS site contains some private material that is (commercially) valuable, like e.g. a diary of a well-known artist. Inheritance law or copyright law may play a role in this case. At least one company is trying to make a business case out of ensuring some kind of digital

122 "Picasa name tags" http://picasaweb.google.com

123 "Teens killed in cyber bullying 'epidemic"' http://www.crime-research.org/news/02.21.2009/3717

124 "British Airways staff attack passengers on Facebook – British Airways passengers are 'smelly and annoying', a group of the airline's employees has claimed." http://www.telegraph.co.uk/travel/3366187/British-Airways-staff-attack-passengers-on-Facebook.html

inheritance (including the SNS profile)[125]. Moreover, dormant SNS profiles of deceased persons may be the object of misuse[126].

[125] "Legacy Locker: Logging off in peace" http://www.telegraph.co.uk/scienceandtechnology/technology/5131134/Legacy-Locker-Logging-off-in-peace.html
https://www.legacylocker.com/

[126] "There's life after death if you're online" http://www.guardian.co.uk/technology/2008/aug/07/socialnetworking.myspace

Chapter 8

Conclusion

This heartbeat provides an analysis of privacy and identity management throughout life. Chapter two gave a brief introduction on identity from a sociological as well as a technical perspective. It is useful to see identity not as a single concept, but rather in the respect of individuals having multiple partial identities that literally come into play in different contexts. We have adopted Roger Clarke's notion of digital persona in this deliverable as the digital representation of an identity. It is useful to distinguish between projected personae and imposed personae. The projected persona is how the individual aims to present himself to the outside world whereas imposed persona relates to the image that others create of an individual. Entities, such as governments and enterprises create extensive imposed digital personae of their citizens and customers.

In order to shed some light on differences in the treatment of individuals and to provide a first glimpse of whether partial identities really exist in the real world or whether governments and enterprises create and use a single (holistic) digital identity of the individual, we have explored four specific contexts. We have started with the common background for all individuals, the state-created general formal identity which unsurprisingly plays a central role in the context of citizen-government relations. Next we have explored the domains of education, health care, and employment. The different areas were explored in general and in more detail for the Netherlands, Germany, Belgium and Poland. Brief explorations were made for France, Ireland, Austria, and Sweden.

The analysis shows that in the Netherlands a unique identifier, the BSN, is commonly used in several settings which, in principle, allows for the construction of a compound identity, instead of the citizen having distinct identities in different areas. In Germany this is not the case. There is even a separation between the different federal states, which all have their own regime in certain contexts. However, all German citizens of age 16 and above are obliged to have a personal ID-card which is used for identification by public authorities. Up to now this card only plays a role in the physical world. In the digital world it is much harder to create a compound identity of German citizens. France and Austria both also have ID cards but no single unique identifier that can be used throughout public administration. Belgium, Sweden, Ireland, and Poland do use unique identification numbers, often combined with ID cards.

In the four formal areas, quite some differences occur. Some countries have national student cards, others do not. The same goes for electronic health cards. The Netherlands has no electronic health card, but is working on a central system, called EPD, which aims to improve health care by

providing access to health records electronically. The system progresses towards a general compound medical identity. In the area of employment, all investigated countries show centralized systems to register people that are unemployed.

The chapter on informal identities showed a number of problems that occur when it comes to throughout life aspects and identity management. The issues can be diverged into three categories, namely; data linking different persons; data about other persons, and; data about dead persons. Data remain available after decease. But already during lifetime, several problems occur because of the increasing (electronic) data exchange and processing, and because data can ever more often be related to more than one person. Also, control is a specific issue. In the case of minors or elderly, control over data can be delegated to others, by law or on a voluntary basis.

This heartbeat has shown that in the context of privacy and identity management throughout life specific issues arise that cannot be solved very easily. A comparison between countries in the areas of government, education, health care, and employment showed that there are still differences between countries when it concerns national ID cards or central registers. However, there also seems to be a tendency towards more centralized systems and mandatory eIDs.