IDIS (2010) 3:267–274
DOI 10.1007/s12394-010-0055-x

Privacy by Design

Peter Schaar

Received: 19 March 2010 / Accepted: 19 March 2010 / Published online: 1 April 2010

Abstract In view of rapid and dramatic technological change, it is important to take the special requirements of privacy protection into account early on, because new technological systems often contain hidden dangers which are very difficult to overcome after the basic design has been worked out. So it makes all the more sense to identify and examine possible data protection problems when designing new technology and to incorporate privacy protection into the overall design, instead of having to come up with laborious and time-consuming "patches" later on. This approach is known as "*Privacy by Design*" (PbD).

Keywords *Privacy by Design* · Electronic health card · Electronic ID card · ELENA

PbD is adjuvant for all kinds of IT systems designated or used for the processing of personal data. It should be a crucial requirement for products and services provided to third parties and individual customers (e.g. WiFi routers, social networks and search engines). Many users have only limited IT skills and hence are not in a position to take relevant security measures by themselves in order to protect their own or others' personal data. Therefore, in connection with these IT procedures, basic protection is always necessary (privacy by default). Moreover, providers have to enable users to better protect their personal data, for example by providing appropriate privacy tools (access controls, encryption, provisions for anonymous use).

The idea of incorporating technological data protection into IT systems is not completely new. Recital 46 of Directive 95/46 of the European Union for example refers to the requirement that appropriate technical and organizational measures have to be taken both when designing the processing system and during processing itself, particularly in order to maintain security. However, PbD goes beyond maintaining security. PbD includes the idea that systems should be designed and constructed in a way to avoid or minimize the amount of personal data processed. Key elements of

P. Schaar (✉)
The Federal Commissioner of Data Protection and Freedom of Information, Berlin, Germany
e-mail: peter.schaar@bfdi.bund.de

data minimization are the separation of personal identifiers and content data, the use of pseudonyms and the anonymization or deletion of personal data as early as possible.

The following examples demonstrate how PbD can help improve data protection:

Electronic health card

For several years now, Germany has been preparing to introduce an electronic health card (*elektronische Gesundheitskarte*, eGK) a smart card with an embedded microprocessor which allows additional functions, in particular verifying one's digital identity within the telematics infrastructure of the health-care sector. The smart card will initially contain the cardholder's administrative data which are already on the magnetic health insurance card. The possibility to store additional data (such as prescription drug records, emergency medical information, electronic patient records) is to be added later.

With the new electronic health card, data protection for patients should at least be no worse than under the current system. The intention is even to improve transparency for insured persons and give them extensive options for using their medical data. Cardholders are to have control over the data in all the applications they choose, and to be able to decide themselves as far as possible how much of their health-related data should be stored on the smart card and in the telematics infrastructure and how it should be used. The smart card is to be designed with technical features giving cardholders the ability to manage their own data and the rights to access that data.

The card and the telematics infrastructure must be simple enough for cardholders to use. Processes suitable for everyday use which enable ordinary users to actively exercise their data sovereignty and rights as patients are a basic prerequisite for introducing the electronic health card and operating the telematics infrastructure.

Efforts to modernize the health-care sector must pay attention to strengthening patient sovereignty and patients' rights and to expanding patients' participation. If the use of IT in the health-care sector were to focus only on improving cost-effectiveness and speeding up processing times while neglecting data protection and patients' rights, it would find little acceptance and would have little chance of being implemented.

This is why the technical processes must be suitable for everyday use by all insured persons, so they can actively exercise their rights of participation and control. In this way, the electronic health card and telematics infrastructure offer the chance to improve access to health data, optimize medical treatment and at the same time enhance patients' control over their own data. The technology used must guarantee lasting compliance with the principles of data protection.

Lastly, the entire technical infrastructure must be oriented above all on benefiting patients. All components, interfaces, services and processes in the health telematics must function optimally and meet the requirements of data protection and data security.

Everyone involved in developing the electronic health card has agreed to abide by the following principles:

(1) **Data sovereignty:** The insured person has extensive control over his/her health data to be processed in the electronic health card or the telematics infrastructure. The voluntary medical applications can be used only with the express consent of the insured person and specific access granted by him/her.
(2) **Voluntary basis:** Health data are to be stored only on a voluntary basis, at the discretion of the insured person. No preferential or discriminatory treatment is allowed on the basis of data access granted or denied by the insured person.
(3) **Extent of data:** The insured person must be able to decide which health data are included and when they should be deleted.
(4) **Data access:** The insured person must be able to decide on a case-by-case basis which service provider (physician, pharmacist, midwife, etc.) has access to which data.
(5) **Right to information:** The insured person has the right to read his/her own data and the right to information about them and all processes concerning them.
(6) **Ability to check:** The insured person must be able to use logs to check who accessed which data and when.

The technical processes currently being tested and the robust security mechanisms built into the smart card and the telematics infrastructure are intended to ensure compliance with these data protection principles and thus also the active participation of insured persons in granting access and managing their medical information and access rights.

Data protection and data security have been taken into account when designing the processes and technology. All the components which are essential to data security—that includes all components involved in encrypting data and ensuring the authenticity of participants—must be certified in accordance with a protection profile of the Common Criteria in order to verify their trustworthiness.

All users—patients, insured persons and members of the health professions—must be able to use the systems securely and easily. Processes for data subjects to actively exercise their rights are to be practical and suitable for everyday use, so that the new technology does not discriminate against anyone (such as elderly or ill persons); among others,

- insured persons cannot be assumed to have technical devices,
- insured persons must be able to use these processes conveniently in the context of treatment, for example at the doctor's office or when filling an electronic prescription at a pharmacy, and
- it must be possible to manage applications and rights using a convenient, standardized and easily understandable interface.

The practicality of a system and its suitability for everyday use is an important criterion for the ability to manage the system and provide effective data protection. All business processes must be understandable and as simple as possible for all involved. This criterion places high demands on the design of applications for insured persons, because all insured persons, not only those with advanced computer skills, must be able to exercise their rights. The generally applicable rule of not

discriminating against persons with few computer skills applies especially to the health-care field. Particularly when designing systems, it is important to make sure that the new technology does not discriminate against elderly or ill persons.

However, the more complex a system and its security functions become (e.g. the length of passwords or PINs, different rights for different user groups), the higher the demands on system participants. After a certain point, such complexity becomes counterproductive: As applied in practice, processes are less effective and less transparent and may create undesirable side effects and new security risks.

That is why it is necessary to clarify in advance how to deal with certain foreseeable constellations in which insured persons are unable to operate the security functions of the electronic health card. This applies to persons with a physical or mental disability, for example, and for persons in extreme situations, such as when the insured person is unconscious and immediate access to certain medical data is essential. One solution might be for cardholders to give their physician the power to manage access rights when they are unable to do so themselves. But even in this case, it is necessary to guarantee that the data subject ultimately decides who has access to his/her data and when.

This is why the design of the system must be carefully planned. Key components of the system are currently undergoing a large-scale test in which system specifications will need fine-tuning, depending on the practical experience gained.

In my view, the electronic health card could become a model for ensuring data protection and data security using privacy-friendly technology, if the design principles listed are consistently implemented. Both the health-care sector and the rights of data subjects could benefit from the new smart card.

However, since the initial rollout of the electronic health card, there have recently been indications that not all participants are willing to bear the costs of the complex infrastructure required by data protection law. For example, certain circles of the medical profession have objected to having to buy new hardware to meet security standards and have called for using software solutions instead, in order to cut costs. I doubt whether the intended and legally mandated security standards can be achieved in this way.

Electronic ID card

Another example of privacy-friendly design could be Germany's new electronic ID card (*neuer elektronischer Personalausweis*, nPA), to be introduced in late 2010.

Given the data protection controversy that arose over the digital passports with biometric features which were introduced a few years ago, this positive assessment may seem a bit strange. In addition to serving as official identification, the electronic ID card will offer the option of electronic identity verification (eID) in a way that takes the requirements of data protection law into account from the very start. This function will make it possible to use the new ID card to verify the cardholder's identity when using Internet services. The new ID card will also offer an optional electronic signature function; like the identity verification function, the electronic signature function will be activated only at the cardholder's explicit request.

The ID card meets key data protection requirements even for the biometric features (digital facial image and fingerprints) which are accessible only to

government officials for the purpose of checking identity. These biometric features are stored electronically on an especially secure part of the chip. And new legislation was passed to make sure that only the digital facial image is mandatory; cardholders may decide whether to have their fingerprints stored on the chip.

Privacy by Design means first of all data security. With the new electronic ID, this takes the form of protected access to biometric and eID data and secure transmission channels. The legally mandated procedure meets most of these requirements, and the components used in the system are to be certified in accordance with uniform security criteria.

But PbD does more than ensure data security; *Privacy by Design* also means collecting and processing as little personal data as possible (principle of data minimization). With regard to the new ID card, this could mean making it impossible to save event and localization data, so that no data-related profile can be created "on" the ID card. Neither past checks of biometric data conducted by government officials nor business contacts using the identity verification function may be retrieved from the relevant zone of the chip and certainly not retrieved and stored by the other zone. This prevents data from being generated when the new ID card is used in different ways and from being used to compile profiles of movement or behaviour.

A good example of *Privacy by Design* could be the possibility to use different pseudonyms for different service providers within the framework of the electronic identity verification function. Cardholders should be able to choose which name they use with which business or public agency (*Privacy by Design* as a role-playing strategy). It is also important for the new ID card to offer a function for verifying the cardholder's age. Age is a prerequisite for certain services (such as those restricted to persons over age 18), and this function allows the cardholder's age to be verified without revealing the cardholder's name, address or even date of birth.

Privacy by Design also means thoroughly analysing and assessing the future vulnerability of originally secure technology (to misuse). In this context, the validity period of certificates should not be set to run too long, for example. In designing technical systems, it is also important to remember that as computer systems become increasingly powerful, in a few years they will be able to decipher encryption and access codes that today seem unbreakable. Other security gaps may become apparent only over time. So the system design must allow for the possibility to optimize or add to certain security features later on.

In a further and more abstract sense, beyond the requirements of Sections 3a and 9 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) in Germany, *Privacy by Design* also means anticipating technological, economic and social developments and how they will interact in order to incorporate data protection for tomorrow into today's IT or, where this is not possible, to limit the lifetime of technology and processes used.

Electronic proof of earnings (ELENA)

The Federal Commissioner for Data Protection and Freedom of Information was involved at a very early stage of planning for a project which has gone since 1

January 2010 by the name of ELENA, an acronym for the German phrase for electronic proof of earnings (*elektronischer Entgeltnachweis*). ELENA is a database in which all the income data of persons employed in Germany will be stored and used to generate electronic proof of earnings to be sent to the social services authority as needed, such as when applying for certain benefits.

ELENA was created to replace the previous procedure, in which an employer uses a specific official form to provide certain income data and other information about the employee applying for benefits. The data are needed to calculate social benefits such as child benefit. Most of these data should be regarded as sensitive and especially at risk of misuse, so their security deserves special attention.

In order to achieve this, special data protection legal provisions from Book X of the Social Code and the Federal Data Protection Act as well as security specifications set by the Federal Office for Information Security (BSI) were taken into account when developing the processes and applications. In addition, the following principles of data protection law were observed:

1. encryption of all transmission channels and all data files in the database;
2. spatial, organizational, technical and personnel separation between the central database and the body responsible for registering participants and processing their data;
3. rigorous separation between the body storing the data and the body responsible for administering the master key. The German Bundestag assigned me, as Federal Commissioner for Data Protection and Freedom of Information, the responsibility of administering the master key;
4. keeping a log of all database transactions, retrievals, etc., in order to document all data processing operations for examination by the data protection supervisory authorities;
5. immediate and targeted deletion of data when they are no longer necessary;
6. internal technical separation and isolation of all organizational units involved in the system, and defining an inner and outer layer of security, each with its own physical barriers and oversight mechanisms;
7. principle of requiring two signatures to retrieve data (the retrieving body and the data subject must always authorize data retrieval by presenting a signature card bearing a legally mandated qualified signature);
8. only authorized agencies and their staff may retrieve the parts of the data file necessary to carry out the task at hand (subject to both content and time restrictions);
9. technical measures to ensure that data are used only for the purpose for which they were collected, and in particular that no access is given to the security authorities, tax authorities, Customs, and the like.

The only way to guarantee that these principles of data protection law were built into this complex system, thereby ensuring the individual's right of privacy, was by involving data protection authorities at an early stage in the planning.

Despite attention to data protection requirements, ELENA faced increasing criticism in the months before its introduction. The criticism initially focused on the quantity of data to be stored centrally—even if encrypted—which had previously

only been kept by employers. This criticism was at least in part understandable and justified.

Although the system design included the highly effective and technically complex protection measures described above, the need for collecting the various data was subject only to cursory examination. The conventional paper forms used until then for proof of earnings statements largely set the standard; as a result, all data elements collected under the conventional procedure were also included in the new ELENA system. It became clear, however, that there was good reason to doubt the need for certain data fields. This experience demonstrated that *Privacy by Design* should not be reduced to ensuring data security and technical data protection functions (such as the use of electronic signature cards and data encryption), and that a process evolves and must meet new requirements.

The example of ELENA also demonstrates that PbD should not be limited to developing clever technical solutions and incorporating them into systems. It is equally important to examine very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary. The tendency to reproduce increasingly complicated bureaucratic systems exactly in information technology can be seen in other IT processes and can lead to major problems for data protection. This risks exists even when great efforts are made to ensure data protection and prevent data misuse.

The *Privacy by Design* principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of IT systems. They should be obliged to take technological data protection into account already at the planning stage of IT procedures and systems. Providers of IT systems or services as controllers should demonstrate that they have taken all measures necessary to comply with these requirements.

When taking decisions about the design of a processing system, its acquisition and operation, the following general objectives should be observed:

- **Data minimization**: Data processing systems should be designed and selected in accordance with the aim of collecting, processing and using no personal data at all or as little personal data as possible.
- **Controllability:** An IT system should provide data subjects with effective control over their personal data. The possibilities for consent and objection should be supported by technological means.
- **Transparency**: Both developers and operators of IT systems must ensure that data subjects are informed in detail about how the systems work.
- **Data confidentiality:** IT systems must be designed and secured so that only authorized entities have access to personal data.
- **Data quality**: Data controllers must support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- **Possibility of segregation**: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing) must guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

The increasing significance of data protection when creating and operating IT systems creates additional requirements for IT specialists. As a result, data protection must be an essential element in the training of IT professionals.