Delegation for Privacy Management from Womb to Tomb - A European Perspective

Marit Hansen, Maren Raguse, Katalin Storf, Harald Zwingelberg

Delegation for Privacy Management from Womb to Tomb – A European Perspective

Marit Hansen[1], Maren Raguse[2], Katalin Storf[1], Harald Zwingelberg[1]

[1]Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Holstenstr. 98, 24103 Kiel, Germany, {ULD6, ULD77, ULD65}@datenschutzzentrum.de
[2]Ministerium für Arbeit, Soziales und Gesundheit Schleswig-Holstein,
Adolf-Westphal Str. 4, 24146 Kiel, Germany, maren.raguse@sozmi.landsh.de

Abstract. In our information society with processing of personal data in almost all areas of life, the legally granted right to privacy is quite hard to preserve. User-controlled identity management systems have been proposed as a means to manage one's own private sphere. Still there is no functioning concept how privacy protection can be effectively safeguarded over a long time period and how self-determination in the field of privacy can be maintained in all stages of life from the womb to the tomb. When user control and the capability to exercise rights can not yet or no longer be carried out by the data subject herself, the decisions concerning the processing of personal data may have to be delegated to a delegate. In this text, we elaborate on delegation of privacy-relevant actions under a lifelong perspective and point out possible legal, technological, and organizational measures to appropriately take up the arising challenges. For crucial gaps in current concepts we sketch solutions and explain implications on user-controlled identity management systems. Finally we give recommendations to stakeholders such as data controllers, application designers and policy makers.

Keywords: lifelong privacy, user-controlled identity management, delegation of privacy, incapability to exercise rights, privacy by delegate

1 Introduction[1]

Since the beginning of humankind, technological progress has led to a change of society. However, in a time of rapid development of technologies and applications it is hard for many people to keep pace with changing trends. Who could have predicted thirty years ago that personal computers, mobile phones, and navigation systems

[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. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

would become part of life of almost every individual in the industrialized world? And who has a clue what our information society will look like in another thirty years? Extrapolating from our quite young experience with information and communication technologies, we see a risk that certain traditional values and concepts – such as privacy protection – which have proven themselves good for a democratic society will be abandoned, probably more or less by accident. This calls for solutions how to maintain one's privacy throughout one's life as it is discussed in [1] and [2].

In this text we focus on privacy aspects of delegation as a means to support individuals in stages of life when they cannot act on their own – from prenatal stages over birth to death, and possibly even a bit beyond. Similarly individuals can be supported who are not willing to act on their own regarding some aspects of their privacy although they might be capable to do it. For a better understanding of the following sections, we give some definitions:

Stage of life: A **stage of life** of an individual with respect to managing her privacy is a period of life in which her ability to do so remains between defined boundaries characterizing this stage of life [1, 2]. Every individual during her lifetime passes through one or more stages during which she is incapable of managing her privacy on her own. Such an **incapability of managing one's privacy** means not having the ability to sufficiently understand the consequences of data processing relevant to one's private sphere or to (re)act upon them appropriately.

Delegation: Delegation is a process whereby a **delegate** (also called "proxy", "mandatory" or "agent") is authorized to act on behalf of a **person concerned** via a **mandate of authority** (or for short: mandate).

The mandate of authority usually defines in particular

(1) the **scope of authority** for the actions of a delegate on behalf of a person concerned and

(2) when and under which conditions the delegate gets the **power of authority** to act on behalf of the person concerned.

The delegate shall only act on behalf of the person concerned if the delegate has the actual power of authority and if his action lies within the scope of authority. The simple acting of the delegate with the existence of a mandate while not having the power of authority would not be sufficient. The difference between mandate and power of authority becomes clear in the following example: In working life the schedule of responsibilities may determine that person A should take over the work of colleague B if the latter is absent. The issuance of the mandate of authority to A is expressed by the schedule of responsibilities, but the A's actual power of authority only comes into existence if B is absent. Otherwise A must not act on behalf of B.

The mandate of authority is issued by the **delegator** (also called "mandator"). This may be the person concerned herself, but there are also cases where other entities explicitly decide on the delegation (e.g., in the case of incapacitation of a person the guardianship court rules on delegation) or where the delegation is foreseen in law (e.g., when parents are the default delegates of their young children). The mandate of authority is usually assigned for a specific period of time. Similar to the process of issuing a mandate, changing or revoking the mandate can be done by the delegator, i.e., by the person concerned herself or by other entities. The conditions and processes to issue, change, or revoke a mandate can be defined by the underlying contract or law.

Note that not always the delegate is aware of the mandate of authority or of the fact that he actually has the power of authority. So the delegator should implement an appropriate way of informing the delegate (and the person concerned if she is not the delegator herself) about the mandate and the power of authority.

For supervising purposes of the delegation and related actions by the parties involved, one or more impartial **delegation supervisors** may be appointed by one or more of the actors. In particular the person concerned may have the need to check whether the delegate really acts as agreed upon.

Delegation has been discussed by various authors, mainly aiming at technical solutions for specific scenarios. Putting the focus on privacy aspects and adding the legal perspective, we deviate slightly from the definitions used in [3] or [4].[2] In our setting, the person concerned is a natural person with some interest in her privacy; the other actors, in particular the delegate, may be natural persons, also caring for their individual privacy.

European data protection legislation: In this text we focus on the European view with respect to data protection and protection of one's private sphere: The baseline of this view is Art. 8 of the European Convention on Human Rights which provides a right to respect for one's "private and family life, his home and his correspondence". Several laws and by-laws substantiate privacy-relevant issues. For EC Member States, the European Data Protection Directive 95/46/EC and further directives in the areas of telecommunication or e-commerce harmonize data protection regulation. The European Data Protection Directive defines the following terms in its Art. 2:

"'personal data' shall mean any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity";

"'processing of personal data' ('**processing'**) shall mean any operation or set of operations which is performed upon personal data, [...], such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction";

"'[**data**] **controller**' shall mean the natural or legal person, [...] which alone or jointly with others determines the purposes and means of the processing of personal data; [...]";

"'[**data**] **processor**' shall mean a natural or legal person, [...] which processes personal data on behalf of the controller".

Note that usually privacy management of individuals is intertwined with actions from other contexts of life (e.g., using a service or communicating with other persons) so that it is difficult to restrict delegation on privacy management only. On the other hand, delegation performed not specifically for the purpose of privacy management very often cannot be separated fully from privacy-relevant issues. For instance if a delegate is handling the financial affairs of a person concerned, this involves personal data of the person concerned, of all financial contacts, and finally of the delegate herself – and all these data can be relevant for managing the private sphere of the

[2] See also Section 5 on related work.

person concerned, and as we will see later, also of the delegate. In the following, we will speak about "delegation of privacy-relevant actions" which encompasses explicit privacy management activities such as the exercise of data subjects' rights as well as other issues which may be relevant to the privacy of the person concerned.

Delegation of privacy-relevant actions to third persons becomes a necessity within any stage of life where an individual is incapable to conduct them on her own, and specifically where she is incapable to care for her privacy needs on her own behalf [5]. After this introduction Section 2 analyzes privacy aspects of delegation. Relevant stages of life (determined, e.g., by childhood, temporary illness, or dementia) together with main legal regulations on delegation, corresponding challenges and possible solutions will be further discussed in Section 3. Section 4 elaborates on recommendations for implementing privacy-aware delegation. Related work is presented in Section 5. Finally, Section 6 concludes the text and gives an outlook.

2 Privacy-relevant challenges concerning delegation

Civil laws around the world provide sophisticated mechanisms on legal kinds of delegation such as representation and agency including a framework of rights for the time when the delegation ends. This might, depending on the legal system, include rules on liability or rules regarding minors' rights to nullify or resign from contracts concluded in their name by their parents. Also protective means against indebtedness of minors reaching maturity are regularly in place.[3] While debts can be legally nullified and contracts cancelled, a transmission of personal data including the resulting consequences once the information has been released may not be revoked as easily, if possible at all. Usually the actions of the delegate on behalf of the person concerned include disclosure of personal data of the person concerned and/or the delegate, so both may have to bear immediate or later consequences to their own privacy. In the following, several privacy-relevant challenges concerning delegation are pointed out.

2.1 Transparency of privacy-relevant actions performed by the delegate

A precondition for managing a person's privacy is transparency on who processes one's personal data for which purpose and under which conditions. This also applies to past transactions or other disclosures of personal data. Getting this information should be easily possible for all individuals concerned, and of course also when involving a delegate. However, in the online world people scarcely know all aspects of data processing which may be relevant to their privacy, e.g., they are rarely aware of data trails like IP addresses or browser chatter in local or remote log files, they have no idea who can access their data on routers or servers, they do not know about profiling algorithms applied to their digital identities. Even in the offline world it is

[3] For example, the German Civil Code (Bürgerliches Gesetzbuch – BGB) limits the liability of a young adult for debts assumed by the legal representatives to the person's assets when reaching majority age, § 1629a BGB.

difficult to be sure who else gets access to personal data disclosed to one data controller because there may be further data processors involved, or the data may be transferred to other data controllers, or there may be a data breach giving access to unauthorized parties.

For online transactions, user-controlled identity management systems have been proposed [5, 6, 7] which – among others – can store privacy-relevant information on past transactions and provide the possibility to later find out about which data the user has disclosed to whom in a former transaction. In the PRIME/PrimeLife project this functionality is called "Data Track" [6]. The data track aims at providing a comprehensive overview of what personal data the user has released to whom, under which partial identity (in particular under which pseudonym), when, and under which conditions (including privacy policy statements such as the purpose, the retention time etc.) [7]. Transferring this concept to delegation entails that one can establish some kind of shared data track which enables the person concerned to know about privacy-relevant actions the delegate performed on her behalf and likewise gives input to the respective identity management systems of the person concerned and the delegate as far as their own partial identities are concerned.

Another solution is to get help from another party which can supervise the delegate's actions: The person concerned could appoint one or more impartial **delegation supervisors** which could see or check all other delegates' actions, but could not act otherwise. For transparency reasons, supervising actions of such a delegation supervisor in general have to be visible for all involved and supervised persons.

2.2 Making actions from the person concerned and the delegate distinguishable

Many of today's services like web shops or online banking applications, or social networks are not designed to support delegates. In particular they don't enable them authentication [8] on their own and expressing the fact and extent of delegation. For services which use knowledge-based authentication mechanisms, e.g., account name combined with a password or PIN, a person concerned is frequently forced to reveal her identification credentials to the delegate who will then act under the name of the person concerned. In case the authentication is object-based and involves, e.g., a hardware token such as a chipcard, the person concerned would have to give this token to the delegate. Often the service's terms of use prohibit the transfer of authentication credentials. For the service it is not distinguishable whether actions are taken by the person concerned or the delegate or an identity thief. In [9] where a typology of various characteristics of "identity[4] change" among different actors is elaborated, "identity delegation" with consent of the "original identity bearer" is dissociated from "identity takeover" without the identity bearer's consent – but these two forms won't be distinguishable for the service when using the same credentials. At least in cases where the person concerned has never granted authority for the measures taken on her behalf and under her name, it becomes a problem if she cannot prove to the service that she didn't act on her own. Then she instead of the delegate

[4] Note that [5] uses the term "identity" also for "partial identities".

would be held liable for the performed actions. This could be avoided when the underlying infrastructure would support that delegates act under their own partial identity, e.g., the person concerned assigns certain rights to the delegate's account or issues specific credentials to the delegate also indicating the scope of the delegate's authority. The introduction of measures that enable delegates to act under their own name should be encouraged by all relevant stakeholders such as data protection commissions, administration, standardization bodies and the service providers themselves.

2.3 Guidelines for the delegate

As people may feel very differently how it should be dealt with their personal data, a person concerned should be able to define preferences and guidelines or even set specific conditions for the use of her personal data. Lawmakers should provide general guidelines how delegates should – when other preferences are absent – treat personal information of an incapable person concerned. However, when a person concerned is able to stipulate certain preferences, she should be enabled to influence the treatment of her (partial) identities to a certain extent, e.g., extroverted persons may allow and encourage the use of their own photographs in social networks, while others may prefer to remain as anonymous as possible.

Applying data tracks raises further questions such as to which data track to write when a delegate exercises the rights of the person concerned under the delegate's name. In such cases both involved persons release personal data and thus could (or should) store this information for future reference. However, both the person concerned and the delegate process personal data about each other – it may even be discussed whether they may become data controllers in the sense of the European Data Protection Directive 95/46/EC themselves [10]. No matter whether it is a legally obliged data controller or another entity processing personal data, the processing entity bears some responsibility for the data which requires the provision of appropriate safeguards. Among others, a deletion period for the data could be indicated and enforced, or for enhancing trust, certain rights on the processing of each other's personal data could be stipulated.

2.4 Balancing the interests of the person concerned and the delegate

While a delegate should be bound to the general guidelines and expressed preferences, these requirements must not be overstrained. Otherwise possible delegates might refrain from volunteering due to fear of liability. Rather a fair balance must be struck with other duties conferred to the delegate, e.g., being an appointed custodian as well. Often delegates will not be professionals in data protection, but rather in a personal stress situation as a near relative or friend became unexpectedly incapable to act on her own behalf and privacy-related considerations are understandably only of minor significance compared to solving pressing problems such as getting a medical treatment or home care.

3 Delegation at different stages of life

The challenges indicated in the previous section and possible solutions for a delegation of privacy-relevant actions may differ and require customization in accordance to the stage of life concerned. These stages and specific legal and factual characteristics are identified in the following.

The approach of user-controlled identity management [5, 7] as well as of exercising informational self-determination presupposes that the acting data subject sufficiently comprehends the effect of the data processing as a question and likewise can act accordingly. Every natural person during her lifetime passes through (a) stage(s) of life during which she does not have the ability to understand the consequences of data processing conducted by data controllers, or she is not capable to exercise her self-determination via the provided means, e.g., due to usability problems. During these phases a data subject needs to be represented by another person who exercises the right on behalf of her. This may start when a child is born, and it may continue in the case of adults that have temporary or permanent needs to get support, and it may finally end with the death of the data subject concerning her last will.

The current civil legal framework encompasses several instruments regulating legal representation or agency which have an effect also with regards to the exercise of fundamental rights: For minors the instrument of parental care is known in civil law. Most of the EC Member States also have legal regulations regarding the representation on children. The Article 29 Data Protection Working Party defined in its Opinion 2/2009 [11] principles regarding children's privacy which we generalize in the following to the relation of persons concerned and delegates regarding privacy-relevant actions:

- The delegate should act in the best interest of the person concerned. This may comprise protection and care which are necessary for the well-being of the person concerned.
- Guidelines for delegation should be defined beforehand.
- The person concerned and her delegates may have competing interests. If conflicts cannot be avoided, it should be clarified how to sort them out, possibly with the help of external parties. Note that a delegate does not necessarily stand in for all partial identities of the person concerned which may lead to additional conflicts of interest of parties involved.
- The degree of delegation should be geared to the capabilities of the person concerned regarding privacy and self-determination. This means that the degree of accountability of the person concerned has to be adapted over time, and regarding privacy-relevant decisions taken by the delegate, the person concerned has a right to be consulted.

It appears that the privacy protection rights of an individual are exercised by different people during the lifetime. This asks for a delegation system where it is clear for all parties involved who can perform which rights at which moment and in which context. The consequences of the delegate's actions may both influence the privacy of the person concerned and the delegate herself to a certain extent.

The following subsections explore various stages of life with respect to delegation.

3.1 Fruit of the womb (“From womb …”)

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

3.2 Children and teenagers

Growing autonomy is an important issue in protection of children’s rights, in any area of law. The complexity of situations involving minors is based on the fact that children, despite having full rights, need a representative to exercise these rights – including their privacy rights. Data protection for children starts within the first days after birth and the processing and storage of birth data or medicine data within the hospital. The protection of personal data of children resides more or less in the responsibility of parents or legal guardians. But when a child grows up, other responsible persons for data processing in different areas of life may become involved, such as teachers, doctors or supervisors [5].

The rights of the child and the exercise of those rights – including that of data protection – should be expressed in a way which recognizes as many as possible of the abovementioned aspects of the situation [11] as follows: until a certain age children have no way to monitor data processing, simply because they are too young to be involved in certain activities. If their parents decide, for example, to put the child’s pictures on their profile in a social network, it is the parents who make the decision about the processing of their children’s data and give the consent to do so on behalf of the child. Normally, putting pictures of another person in a social network profile requires consent of that person, the data subject. In the situation described here, the parents are entitled to express the consent in the name of the child. Such a situation may put the parents in the double role – of data controllers while publishing their child’s personal information open on the web, and, at the same time, of consent issuers as the child’s representatives. This double role may easily lead to conflicts. Parents must take great care not to cross the line of the child’s best interest when processing the child’s data.

It is necessary for the parents or other representatives to listen carefully to the interests of the child at least beginning from a certain age and consider those interests when making a privacy-relevant decision as that decision is binding for the child [11]. When the child reaches legal age and becomes an adult, it may want to change the recent decision of the parents. Therefore the child needs to know what decisions about processing of personal data were made by the representatives. Afterwards the child needs to give her explicit consent for the processing of personal data. This may be implemented in certain operations in a way that the operator is reminded that the

person of legal age[5] and now the explicit consent is needed. This is relevant in many circumstances, e.g., medical matters, recreational activities of the child, school matters, or agreements made by the parents before the child's majority.

As children and teenagers are in the process of developing physically and mentally, the rights of the child and the exercise of those rights – including the rights of data protection – should be accomplished in a way which recognizes these aspects of the situation. Especially the adaptation of the degree of maturity of children and teenagers is a central aspect that has to be taken into account by their parents. Children gradually become capable of contributing to decisions made about them. It is natural that the level of comprehension is not the same in case of a 7-year-old child and a 15-year-old teenager.[6] This in particularity has to be recognized by the children's representatives. Therefore the children should be consulted more regularly about the exercise of their rights, including those relating to data protection.

The children's representatives should also think about a way to document privacy-relevant decisions so that when the children have become teenagers or young adults they can easily understand what personal data have been disclosed to whom and under which conditions. This would enable the grown-up children to actively approach certain data controllers to give or revoke consent concerning data processing or to request access, rectification or erasure of their personal data.

3.3 Adults lacking privacy management capabilities

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

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

---

[5] The definition of "legal age" of a person and the corresponding age in years differs within Europe. There are different categories of legal age, such as age of consent with respect to sexual activities, age of criminal responsibility, legal drinking age, marriage age, voting age or age of majority. The age of majority is in general the threshold of adulthood and defines the chronological moment when a minor ceases to legally be considered a child and assumes control over their personal actions and decisions. The age of majority means terminating the legal control and legal responsibility of the parents or other guardians. In the European Members States the age of majority is set to 18 years.

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

3.4 Deceased people ("… to tomb")

In situations where a person has died, the instrument of law of succession applies. The European Data Protection Directive 95/46/EC assigns the right of privacy and data protection to "natural persons" (Article 1). Deceased persons are no longer regarded as data subjects. Protection against an unregulated processing of data concerning deceased individuals in some European legal frameworks[7] is provided by means of a "post-mortal personality right". In some situations, the instrument offered by the law of succession might not be sufficient – further regulations are needed.

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

Meanwhile new services appear on the market which offer to send out secure messages to friends after the death of the user. Their goal is to give people a safe way to share account passwords, wills and other information. When users book the service against payment of a fee, they get options for when to send messages or to delete some messages permanently after their death. As already shown in Section 2.2, it is problematic if authentication credentials of the user have to be transferred to the service which opens the way to misuse because it is not distinguishable for others whether the user or the service acts.

4 Recommendations for implementing privacy-aware delegation

As in the networked world oblivion of negative facts is hindered or impossible and even neutral information may turn against the data subject years later, it had been our initial assumption that a need to provide for lifelong measures in respect of privacy rights exists [2, 5]. Measures must be taken urgently as also the current use and collection of data may have negative future implications on data subjects. This is not only necessary for persons who can handle their privacy interest on their own, but even more so for persons who are currently or permanently incapable to preserve their rights. In periods of incapability it becomes necessary that third persons act on behalf of the person concerned and that, if adequate, the person concerned may choose and instruct her delegates herself. Regarding privacy-aware delegation we derive a set of

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

technical, legal, and societal recommendations and finally adapt our reflections on user-controlled identity management systems.

4.1 Recommendations for data controllers and application designers

Allowing delegation within the field of privacy requires that some preconditions are met from the involved technologies and underlying processes [5]. Implementing these is a task that is best addressed by data controllers and application designers as these stakeholders have control over the relevant technology and processes in their specific application setting. Data controllers, such as service providers, are responsible for the actual data processing and choose for that an implementation provided by an application designer. In the procurement process, data controllers should ask for the recommend functionality which should be provided by application designers. The implementation lies also within the well understood interest of these stakeholders, e.g., as the measures can increase security and especially accountability and legal enforceability of the data controller's transactions. The following measures should be implemented:

- **Technical representation of delegation:** Usually delegation is expressed by issuance of a "mandate certificate" to the delegate. Among the important procedures to be specified are: issuance of the mandate of authority to the delegate, activation of the actual power of authority, conducting actions under the name of the person concerned within the scope of the authority, verification of the authority, revocation of the authority from the delegate, and expression of acceptance of the mandate by the delegate [12]. For all these procedures it is important that they ensure the necessary level of security to prevent misuse.
- **The credentials of the person concerned must not be used by the delegate:** Delegation has to be enabled without transferring the original credentials (such as tokens or certificates) of the person concerned to prevent identity theft. Possible implementations include derived credentials for delegates or that the delegate uses own credentials to get access and then indicates that she acts in behalf of the person concerned.
- **Logging:** Actions taken by a delegate must be traceable by the person concerned or on her behalf.
- **Preferences and conditions:** Where possible, the person concerned should be enabled to define the scope of authority by declaring preferences and conditions, e.g., to partially or absolutely restrict certain disclosures, to stipulate preferences or by giving guidelines for data usage in form of preferences but allowing exceptions for transactions she is interested in regardless of the data required. The application should support both expressing these preferences and conditions and checking whether they have been adhered to.
- **Protection of the delegate's privacy:** The delegate's own desires for maintaining his privacy have to be considered in addition to the privacy requirements of the person concerned. Here **data minimizing** solutions, e.g., by anonymous authorizations, can help preserving the private spheres of both parties involved.
- **Supervision of the delegation:** As exercising privacy and other personal rights is a strictly individual decision, a person concerned should be enabled to choose one or

more impartial delegation supervisors trusted by the person concerned to look after her interests. This is in particular necessary when a delegate was appointed by a third party (e.g., by a court).

- **Stipulations for post-mortal period:** Where applicable, as personal data will be processed and particularly distributed after a person's death such as in social networks, data controllers should clarify the use of such data in their privacy policies after the user's death. Users should be enabled to stipulate preferences for the post-mortal processing of their personal data.

4.2 Recommendations for policy makers

Several legal prerequisites are necessary to lay the foundation for effective and privacy-aware delegation. These requirements address policy makers such as parliaments for providing a solid legal foundation, but also standardization bodies and data protection authorities for ensuring practicability and consistent enforcement.

- **Delegation in privacy issues should be recognized by law** as far as legally possible, e.g., requiring actions in person only where private law acknowledges similar requirements (like the requirement that a will cannot be made by a delegate could correspond with a regulation that privacy rights for the post-mortal period require a specific written authorization). It must be compulsory for data controllers to accept declarations made by a delegate on behalf of a person concerned. Concerning the legally granted data protection rights of data subjects such as the "right of access", the "rights to rectify or to delete", and the "right to object", the "Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data" [13] already states that data subjects should be able to exercise those rights "through a representative who shall satisfactorily establish his/her status to the responsible person". Thereby the proof of the identity of the person concerned and her consent as well as the mandate must not be too complicated or costly. Until a reliable eID infrastructure is available, policy makers should provide a respective means for offline use, e.g., with a harmonized form.
- **Delegate not acting under the (partial) identity of the person concerned:** Acting as a delegate should be done under the name of the delegate, under pseudonym, or anonymously while indicating the authorization of the person concerned to act on her behalf.
- **Supervision by the person concerned:** To enable the person concerned to supervise actions taken in her name, certain prerequisites must be met to enable a later revision of privacy-relevant actions in a manipulation-resistant log (e.g., in a shared data track). This supervision has to be transitive if the delegate herself has commissioned other delegates as her own stand-in. As a further consequence the person concerned should also be able to directly exercise her right of access with any data controller – without involving their regular delegate(s). Also minors should be enabled to get professional advice.
- **Specific legal regulations:** In accordance with the suggestions of the Article 29 Data Protection Working Party [11] we suggest that national legislation and interpretation of data protection law should consider minors and other persons

incapable to exercise their privacy rights. Such a regulation should provide guidance and boundaries for delegates.

- **Protection of the delegate:** As persons that are (temporarily) incapable to act on their own with respect to privacy rights are dependant on delegates to act on their behalf, it is necessary that delegates are available. This requires that being a delegate does not comprise too many risks as otherwise only a few persons would volunteer for the task. Policy makers could contribute to this by limiting the liability of delegates. In addition, it would not be proportional to track each action of a delegate in detail as the delegate's privacy may be concerned, too. Here the interests of the person concerned and the delegate have to be balanced in a fair way.
- **Best practices for authorizations of delegates:** Data protection authorities or standardization bodies may provide for a set of predefined authorizations of delegates including definite descriptions of the respective scope of authority. This could possibly give start to research on a whole ontology of the types and causes for delegation and possible limitations of the scope of the authority necessary to comply with the cause's specific needs.

4.3 Societal recommendations

Besides these legal and technical requirements for delegation it is necessary to raise awareness for privacy-related issues in the broad public beginning by including specific privacy-related topics in the curricula for school students. However, considering that parents act as delegates and that sports clubs and schools also publish information on minors, these groups bear high responsibility for data disclosures, underlining the need for specific awareness raising programs in these groups as well.

Teachers, doctors, trainers and other caretakers often take the position of factual delegates, temporarily representing the children's interests within a certain area of life. Here also self-determination and transparency are necessary as soon and as far as possible, requiring a communication with appointed or self chosen delegates of the person concerned. Such factual delegates should handle disclosure of personal data as restrictively as possible and acquire consent of the competent delegate. Especially these caretakers should work on empowering at least those who are only temporarily incapable of handling privacy-relevant actions instead of making themselves indispensible and provoking a lock-in effect.

4.4 Implementing privacy-aware delegation in identity management systems

For the implementation of user-controlled identity management systems the aspect of lifelong privacy also imposes specific requirements. As shown for the example of data tracks, which offer transparency for the person concerned, such technology imposes new challenges (see above Section 2.3).

- **Logging:** Actions taken by a delegate must be traceable for the person concerned (see Section 4.1) e.g., by writing into a data track accessible for both the person concerned and the delegate or by providing copies of the relevant entries. Also the

data track of the delegate should indicate the fact of having acted as delegate and which data was released. However, in case of minors as persons concerned the logging requirements must not overstrain the capabilities of average parents.

- **Control over partial identities:** It must be possible for the person concerned to control which delegate can access and see specific partial identities.
- **Access to the data of the person concerned by the delegate:** Identity management systems should offer a possibility for persons concerned to grant access for data track entries and possibly additional data relevant for the situation to delegates. A delegate may need to base decisions on previously released data or to choose among partial identities of the person concerned in order to avoid linkability of such identities of the person concerned. This includes the possibility of access by delegation supervisors chosen by the person concerned. When allowing access to data tracks, it must be well considered whose track to use and which information should be visible as person concerned and delegate reveal personal data.
- **Support in supervising delegates:** Specific delegation supervisors should get access to all transactions performed by the delegates of the person concerned wishing for such an external supervision. For transparency reasons such accesses should be logged and visible for the supervised persons. The delegation supervisors should not have the access rights to perform any actions except for controlling the delegates of the person concerned. Another controlling effect may be achieved if persons concerned choose multiple delegates which have to agree (or vote) on important decisions before taking action. Again, this would have to be reflected in the identity management systems.
- **Defined retention periods:** A predefined **deletion time for (partial respectively shared) data track entries** could be useful so that only those parts prevail that are necessary for further privacy management. In particular, data track entries which comprise privacy-relevant information for both the delegate and the person concerned may be cut apart, the person concerned may check the delegate's actions on the basis of the logged data, and then only the parts belonging to the person concerned may be kept.
- **Stipulations for post-mortal period:** Identity management systems should provide for a solution to store instructions in case the person concerned dies. This information must not be accessible by the delegates except for the case of explicit clearance by the person concerned or the death of the person concerned.

5 Related work

As a matter of course, various topics in the privacy debate have delegation aspects, e.g., when discussing data protection issues in the health area (whether it be usable health cards, remote medical technologies, or ambient assisted living) or in labor relations (privacy rights of employees, stand-ins for absent colleagues, or representation of the organization as such). On the other hand, numerous publications [12, 14-17] deal with components of delegation from the technological perspective, elaborating specifics of access control, policy interpretation, or cryptographic

certificates. In this section we limit our scope to those papers which contribute to implementing the vision of privacy-aware delegation.

Some delegation schemes were proposed explicitly for federated identity management systems, taking at least some privacy considerations of the user into account [14, 15]. In these papers, the delegate usually is not a natural person, but a provider or service component which acts on behalf of the user. A more generic and distinctly user-centric approach which considers also some legal demands (e.g., deals with the necessity of revocation) has been developed in [12]. The specific scenario of introducing a delegate as mediator between users and service providers which takes care of specific privacy issues of the persons concerned has been proposed in [16] and [17] – here the combination with anonymous credentials and an identity management system shows some similarities to the work on user-controlled identity management [5]. However, none of the approaches deals with persons concerned who are (temporarily) incapable to manage their private spheres and their need to be supported by delegates, and none considers potential desires or privacy rights of the delegate. And even papers that mention identity management do not present solutions how entries of logging components such as the different data tracks involved should be treated.

Further, specific research on aspects of lifelong privacy, arising problems, and possible solutions is ongoing research within the PrimeLife project resulting in a set of derived requirements for a lifelong privacy protection [2].

6 Conclusion and outlook

We have shown that delegation is a necessary prerequisite for preserving lifelong privacy as in every individual's life there are stages of incapability to cover. However, at present many privacy-related technologies lack proper handling of delegation. Providing proper means to enable delegates requires not only further research and development in the field of information and communication technologies, but also a legal framework to establish the basis for handling privacy-aware delegation. As could be shown for delegation and the application of data tracks – a necessary and useful technology in the field of user-controlled identity management – new problems arise by introducing delegates to such systems that must be addressed by a cooperation of legal and technical experts.

Delegation will be valuable and necessary for firstly the ageing population because in the older age the need for support in many areas of life grows. Secondly, common ways of delegation in the working life, like representing a company or covering for a colleague, should consider privacy-relevant matters when being implemented in technology. Thirdly, delegation issues affect the young generation and their parents very much in daily life – with or without a proper implementation in identity management.

Acknowledgments. The authors are thankful for the constructive and very valuable comments of the anonymous reviewers and the vivid discussion among the participants at the Summer School 2009 concerning this topic.

References

1. Clauß, S., Hansen, M., Pfitzmann, A., Raguse, M., Steinbrecher, S.: Tackling the Challenge of Lifelong Privacy. In: Cunningham, P., Cunningham, M. (eds.): Proceedings of eChallenges 2009 (2009)
2. Storf, K., Hansen, M., Raguse, M. (eds.): Requirements and Concepts for Identity Management throughout Life. Deliverable H1.3.5 of the FP7 project PrimeLife, Zurich/Kiel 2009, http://www.primelife.eu/results/documents/ (2009)
3. Pham, Q., Reid, J., McCullagh, A., Dawson, E.: On a Taxonomy of Delegation. In: Gritzalis, D., Lopez, J. (eds.) SEC 2009. IFIP AICT 297, pp. 353--363, IFIP International Federation for Information Processing, Springer, Boston, USA (2009)
4. Crispo, B.: Delegation of Responsibilities. In: Christianson, B., et al. (eds.) Security Protocols. LNCS, vol. 1550, pp. 118--124, Springer, Berlin, Heidelberg, Germany (1998)
5. Hansen, M., Pfitzmann, A., Steinbrecher, S.: Identity Management throughout One's Whole Life. Information Security Technical Report 13, 2 (May 2008), pp. 83--94 (2008)
6. Hansen, M. Fischer-Hübner, S. Pettersson, J.S., Bergmann, M.: Transparency Tools for User-Controlled Identity Management. In: Cunningham, P., Cunningham, M. (eds.) Expanding the Knowledge Economy: Issues, Applications, Case Studies – Proceedings of eChallenges 2007, pp. 1360--1367, IOS Press, Amsterdam, The Netherlands (2007)
7. Leenes, R. Schallaböck, J., Hansen, M.: PRIME White Paper V3 – Privacy and Identity Management for Europe. https://www.prime-project.eu/prime_products/whitepaper/ (2008)
8. O'Gorman, L.: Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, Vol. 91, No. 12 (Dec. 2003), pp. 2019--2040 (2003)
9. Leenes, R. (ed.): ID-related Crime: Towards a Common Ground for Interdisciplinary Research. FIDIS Deliverable D5.2b, Frankfurt, Germany. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp5-del5.2b.ID-related_crime.pdf (2006)
10. Article 29 Data Protection Working Party: Opinion 5/2009 on Online Social Networking. Working Paper 163. 01189/09/EN, adopted on 12 June, 2009, Brussels, Belgium. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf (2009)
11. Article 29 Data Protection Working Party: Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools). Working Paper 160, 398/09/EN, adopted on 11 February, 2009. Brussels, Belgium. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf (2009)
12. Peeters, R., Simoens, K., De Cock, D., Preneel, B.: Cross-Context Delegation through Identity Federation. In: Brömme, A., Busch, C., Hühnlein, D. (eds.) BIOSIG 2008. LNI, vol. 137, pp. 79--92. GI, Köllen Verlag, Bonn, Germany (2008)
13. Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data. Madrid Resolution of the 31st International Conference of the Data Protection and Privacy Commissioners, adopted on 5 November, 2009, https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf (2009)
14. Gomi, H., Hatakeyama, M., Hosono, S., Fujita, S.: A Delegation Framework for Federated Identity Management. In: Proceedings of the ACM CCS 2005 Workshop on Digital Identity Management, pp. 94--103. New York, NY, USA (2005)
15. Alrodhan, W., Mitchell, C.J.: A Delegation Framework for Liberty. In: Haggerty, J., Merabti, M. (eds.) Proceedings of the 3rd Conference on Advances in Computer Security and Forensics (ACSF 2008), pp. 67--73. Liverpool, UK (2008)
16. Wohlgemuth, S., Müller, G.: Privacy with Delegation of Rights by Identity Management. In: Müller, G. (ed.) Emerging Trends in Information and Communication Security (ETRICS) 2006. LNCS, vol. 3995, pp. 175--190. Springer, Berlin, Heidelberg, Germany (2006)
17. Wohlgemuth, S.: Privatsphäre durch die Delegation von Rechten. Vieweg+Teubner, Wiesbaden, Germany (2008)