Data Protection by Default in Identity-Related Applications

Marit Hansen

Data Protection by Default in Identity-Related Applications

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
marit.hansen@privacyresearch.eu

Abstract. "Privacy by default" is being discussed as one important principle for ICT system design. This principle has been taken up as "data protection by default" in the proposal for a European Data Protection Regulation published in 2012. However, it is debated what this principle should mean in practice. In this text, we analyze the relation to "security by default" and "privacy by design" and discuss different possible interpretations of the "data protection by default" principle. After presenting general considerations on how to choose and implement appropriate default settings, we exemplarily describe recommendations for typical identity-related application scenarios such as social network sites, user tracking on the web and user-controlled management of one's identities. Both the general and the scenario-based elaborations provide guidance for developers as well as evaluators.

Keywords: Data Protection by Default, Privacy by Default, Privacy by Design, Security by Default, Identity, Identity Management.

1 Introduction

For several years, data protection authorities and other privacy advocates have been demanding "privacy by default", often in combination with "privacy by design" for conceptualizing, developing and operating ICT systems that are used to process personal data [1]. The general idea of "privacy by design" is to design technologies and business practices right from the beginning according to privacy criteria, thereby implementing important privacy guarantees and features in ICT systems and processes. "Privacy by default" addresses on the one hand that "privacy by design" should be a matter of course in ICT development and operation. On the other hand it defines the goal for a privacy-friendly standard configuration so that the usage of the ICT system does not infringe people's privacy. However, the exact interpretation of "privacy by default" is being debated.

The proposed European Data Protection Regulation [2] has taken up the principles of "privacy by design" and "privacy by default". Since the legal text focuses on "data protection" rather than "privacy" – entirely in the tradition of the European data protection framework in force –, it consequently has incorporated the principles under the names "data protection by design" and "data protection by default". Even without

statutory "data protection by design and by default" on the European level, in some European Member States national data protection law took up these principles at least partially, e.g. in the German telemedia law and the data protection law. In addition, they became criteria of the Schleswig-Holstein Privacy Seal [3] and the European Privacy Seal [4]. Standard settings are clearly relevant when assessing privacy properties of ICT products and services, because they will decide on the effort for users to apply the appropriate configuration for a privacy-compliant use. This is both relevant for users on behalf of an organization – they have to consider the legal requirements when processing personal data – and for end-users for their personal purposes, e.g., when joining a social network. The importance of defaults in ICT design has been explored by various researchers (e.g. [5] and [6]): They conclude that many users stick with the preconfigured settings which might put them unexpectedly at risk.

Not only European data protection authorities, but also the consumer organization BEUC regarded "privacy and security by design" and "privacy and security by default" as important principles that could be already derived from current law [7], in particular from Art. 17 of the European Data Protection Directive [8] that demands "appropriate technical and organisational measures" to protect personal data.

In this paper, we focus on "data protection/privacy by default". The following section describes how "data protection by default" is regarded in the proposed European Data Protection Regulation and what other definitions are being discussed. Section 3 presents general considerations for applying "data protection by default" in practice. In Section 4, recommendations for default settings are shown for three identity-related application scenarios. Section 5 summarizes the findings and gives an outlook.

2 Towards a definition of "data protection by default"

Starting point of this paper is the proposal for a European Data Protection Regulation [2]. In Art. 23 para. 2, "data protection by default" is introduced: "The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals." [2]

This should be read together with recital 61: "(61) The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default." [2]

Firstly, it is noteworthy that rather than ICT developers this provision addresses the controller only, i.e., the entity that "determines the purposes, conditions and means of

the processing of personal data" (Art. 4 para. 5 of the proposed Regulation [2]). Nevertheless, the preconfigured settings are often determined by the ICT developers. Of course, there might be an indirect effect on ICT developers if controllers demand "data protection by default" [9]. However, it would be more appropriate to define an obligation for data controllers, data processors and producers of data processing systems as proposed in the Draft Report of the European Parliament [10].

Secondly, the meaning of "data protection by default" is not clear. The last sentence of Art. 23 para. 2 on accessibility "to an indefinite number of individuals" points to social network sites and other Internet services. Apart from that, the meaning seems to be reduced to the necessity principle (see also Art. 5 (c) of the proposed Regulation [2]): processing of personal data is only allowed if and as long the data are necessary for the purpose. Also, the European Data Protection Supervisor (EDPS) has demanded further clarification: "The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context. The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it. The data subject should in principle be left the choice to allow use of his or her personal data in a broader way. The EDPS recommends including in Article 23(2) a reference to this position of the data subject and providing the necessary clarification in recital 61." [9]

As a contrast, in her work on "privacy by design" Cavoukian does not refer to "least privacy intrusive", but regards "privacy by default" as "privacy as the default setting": "If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default." [11] This sounds good, but if, e.g., the purpose of the application is to disclose personal data to others (as for social networks), an absolute privacy protection cannot be achieved while keeping the functionality. In this case, the EDSP reference to a "simple use" with least privacy infringement probably fits better to the users' expectations.

It is widely agreed that a preconfigured setting does not constitute a user's consent – she might not even be aware of the setting. Also it is out of the question that a user should be able to change the configuration. However, it is debated whether "privacy by default" demands a preconfigured setting. Commissioner Reding, who criticized that "[p]rivacy settings often require considerable operational effort in order to be put in place" [12], focuses on lowering the threshold for users to configure the system according to their needs: privacy settings would have to be "designed to be easily found and manipulated by the user" (Reding according to [13] on "privacy by default"). In this interpretation, "privacy by default" would not need a preconfigured setting, but instead users could be forced to set the configuration at the install or first use of the system. The part of Reding's speech on "privacy by default" recognizes that the use of personal data for other purposes than specified could "be allowed with the explicit consent of the user or if another reason for lawful processing exists". This could mean that the default setting already foresees possible legitimate interests of the controller – other than maximizing the user's privacy – and can only be overridden by

an explicit choice (opt-out) of the user. Frankly speaking, "opt-out" is not what users understand by "privacy by default".

In another way, the proposed Regulation falls short: the limitation to the necessity and data minimization principle. The Draft Report of the European Parliament extends that dividing "data protection by default" into two categories: the default by the controller when the data subject is given a choice, and the default of applying "data protection by design" by data processors and producers to ensure that the privacy-compliant use by controllers [10]. For the latter case, that report relates it to all "principles relating to personal data processing" as introduced in a broadened version of Art. 5 of the proposed Regulation by explicitly mentioning transparency, purpose limitation, data minimization, integrity, storage minimization, intervenability, and accountability [10].

This seems to be a good approach to converge the discussion on "privacy by default". After all, the related – and often overlapping – concept "security by default", together with "security by design" or "built-in security", has been discussed for decades. The information security community has not agreed upon one single definition. But indisputably the well-known standard rule "deny by default" for firewalls is a good example: "firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy" [14] – note that the default "deny all" means that no network traffic can pass, so even a "simple use" would not be possible, and the art of good firewall rules requires skilled engineers. Another possibility of "security by default" is realized by hardening ICT systems, i.e. all "services and features that are not widely needed should be disabled by default or accessible only to a small population of users" and "software should run with the least necessary privilege" [15]. Further, encryption as default, e.g. HTTPS as default for web browsing instead of making it an opt-in feature, is mentioned as an example for "security by default" [16].

Summarizing, "data protection by default" should encompass not only privacy by design as a default, but also least privacy-infringing (or maximally privacy-enhancing) default settings where this is reasonable. The question of defaults should address data controllers, processors and producers.

3 Applying "data protection by default" in practice

In ICT design, "data protection by default" addresses those cases where different configurations are possible, usually depending on the user's choices. For applications that cannot be configured differently, it is demanded anyway that they are legally compliant, and – if the "privacy by design" approach is followed – that they not only respect, but promote the data subject's privacy.

There is no universal answer to when configurable settings should be used and when wired-in functionality without an option to adapt should be preferred. Wired-in functionality may be regarded over-protective or even invasive for the autonomy and informational self-determination of the individual – both important core values of privacy protection. If configurable settings are chosen, their granularity has to be

determined: On the one hand, fine-grained controls may be more appropriate to reflect any situation. On the other hand, they might be too complex for users to understand their meaning and the impact of modification. This would increase the risk of undesired consequences when changing the settings [17]. This usability issue is also raised by companies who fear that "privacy by default" could result "in software design that confuses and annoys customers with repeated notices and warnings." [18] However, this argumentation is inexplicable since "privacy by default" aims at the opposite.

Kesan and Shah [6] describe a framework for setting defaults, specifically for software, and the role of policy makers: In general, they don't recommend policy makers to intervene when developers choose the default settings – as long as they choose a setting that all parties would have agreed upon. However, they do see a need for interference of policy makers in three cases: "when users lack the knowledge and ability to change an important default setting" (this category may also comprise settings unexpected by the user), if the default settings "cause harm to third parties" or if it "does not comport with existing law and policy" [6]. In severe cases, they regard it as "necessary to change the setting from a default value to a wired-in setting" [6]. Especially in the area of privacy, one or more of the listed conditions for policy makers' intervention will often apply concerning today's standard software configuration and the lack of expertise and risk awareness of many users.

When discussing the right defaults, two different types of configuration should be distinguished:

1. The configuration of an additional process that is not strictly needed for the original functionality of the application or its simple use. This is usually associated with a new purpose (e.g. an additional subscription of a newsletter or additional data transfer to other parties that analyze the data). This additional process may be perceived as useful by the data subject, or not.
2. The configuration of a process necessary for the purpose within the application – here it has to be determined how the default setting should be. For instance, in a case where some data have to be transferred, it could be encrypted by default or not. Another example would be how the indubitable payment process for some goods or services is handled, e.g. via prepayment, credit card or direct debit.

The default for the first configuration type is quite clear: For each additional purpose, process or party getting access to personal data the default setting should be "No". Also for some original purposes like disclosing data to friends in social networks, meaningful privacy defaults could limit the risks.

This second configuration type needs more thorough elaboration: It often depends on the functionality that is supported at the user's side; it frequently needs the user's awareness or even consent. For example, the user requires transparency on the payment provider for organizing the money transfer, and usually wants to choose according to her own needs. Here a default would not be demanded. Also, it is not clear which payment method would suit the user best: prepayment, anonymous e-cash, or separated providers that keep financial data confidential and won't gain information on the purchased goods. Further, different methods may result in different costs for the user. Here transparency is needed, but not a one-size-fits-all default.

Concerning encrypted data transfer, thanks to the SSL support in all browsers this can and should be the default for web requests. But for e-mail encryption, this could only be a default if sender and receiver use the same crypto system. Note that some security or privacy functionality, like encryption, may cause performance losses. With today's machines, it is mostly negligible for SSL, so it does not constitute an obstacle against the default setting. Further, legal restrictions for specific countries have to be considered: Even if the privacy default should be a clear "Yes" for well implemented encryption, this may put the user – or the producer – at some legal risk.

In general, the desired privacy default might not be the same all over the world. Think of an application that allows the user to store data in a cloud. According to European data protection law, personal data from Europe shall not be transferred to locations where no adequate level of protection for the rights of the individual is guaranteed. Indeed, undesired access to data demanded by the local government is discussed as one of the major risks when using foreign cloud services. So, a software tool that provides different options for storage locations may have the default setting "Use the European cloud". But should this also apply to non-European users? Probably not – users and policy makers from other nations may prefer a cloud within their territory. In this case, the software could first – in a legally compliant way – analyze the geolocation of the user's IP address to find out whether she comes from Europe and then determine the default setting. However, the exact location of data processing and the place of jurisdiction can be very relevant for a user who wants to assert her data subject's rights, to know about additional risk (e.g. whether the location falls under a data retention regime) or to file a lawsuit.

The solution would be to foresee defaults like that, but to make sure that users notice them and can get more information on the setting, the reasoning behind and possibilities to change the default value. Of course, this would be necessary, too, if costs for the users differ depending on the chosen option. Here it might be better to do without a default, but be explicit on costs and conditions, especially if more security and better privacy protection cost more.

The information on the defaults should always be accessible, even if the user doesn't feel a need to change them. This is not only demanded by transparency requirements, but is also a good means to help users in understanding the system and be able to debate whether the preconfigured defaults are the right ones or should be adapted – not only for the individual, but for a bigger user group.

Not only location can constitute different desired defaults. A special case is the legal requirement for stricter protection of children data. Also, there might be user groups with individual needs, e.g. based on cultural differences or because of disabilities. However, determining the appropriate default is not a compelling legal reason for a comprehensive analysis of personal data at the controller's side. For client configurations at the user's side, it is possible that the user can choose at install or first use between various categories to get the most appropriate defaults, but this must not result in a transfer of potentially sensitive data (e.g. on disabilities).

In addition, there might be "configuration providers" offering the most appropriate default for their respective community, e.g. as a downloadable file or a newsfeed with updates. This may be a data protection authority, a consumer organization, an associa-

tion of people with disabilities, a church, a club or other interested users. These configuration providers could support users if a reaction on a security breach is necessary ("from now on no further data transfer to XY", "abstain from broken crypto algorithm XZ"). By this, more flexibility in shorter reaction time could be achieved. Note that, by providing this default setting, the responsibility and liability for at least that part of the configuration is shifted from the producer/controller/processor to this configuration provider.

From the previous discussion and the legal data protection framework, criteria for assessing potential default settings are sketched in form of a flowchart in Fig. 1.

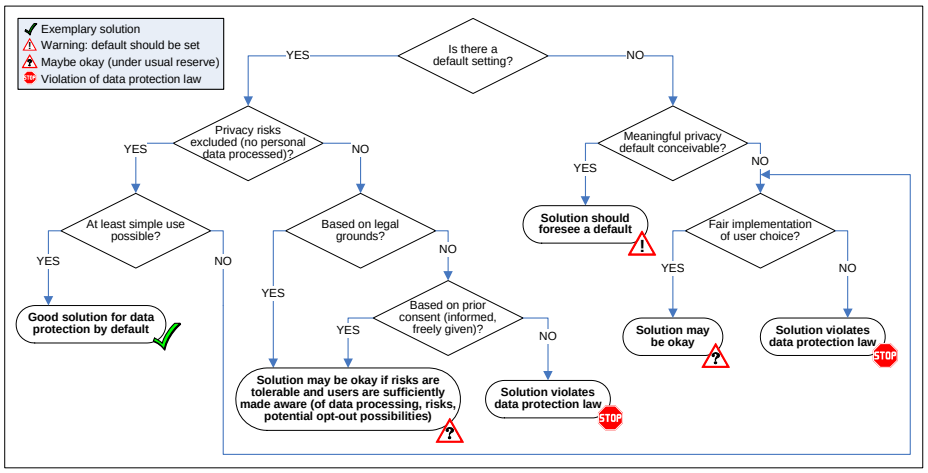

Fig. 1. Assessing potential default settings for user choices in applications.

Clearly, a default setting that excludes any risks and enables an at least simple use of the system is a good solution for data protection by default. However, exclusion of any privacy risk may lead to a severe restriction of functionality to that even a simple use is not possible. In some cases, this can be the best choice to guarantee that users become aware of configuration options – it is comparable to the "deny all" firewall rule that forces the users to think about what they really need.

However, there may be another solution that does not rule out any privacy risk, but is based on legal grounds. Hopefully, these legal grounds are not overly privacy-infringing themselves (think of the data retention directive). An example is the legal provision on pseudonymous profiling of users under strict conditions as foreseen in the German Telemedia Law and in the Draft Report of the Parliament [10]. In this case, the law has defined that users have to be notified and can opt-out, but the default setting may be "Yes" for pseudonymous profiling, although this would not be the least privacy-infringing solution. So it is debatable whether this legally compliant solution still counts as "data protection by default". The reasoning behind privileging pseudonymous data processing is that the purpose can be achieved by accepting a reduced risk compared with a detailed analysis under real names, no matter whether the otherwise legally demanded consent is collected or not. In general, a risk may be

tolerable if it is known to the data subject and no overriding legitimate interests of the data subject would be adversely affected. The same line of thought can be applied if the default relies on a consent the user has given earlier.

As stated above, there are many situations where a meaningful privacy default cannot be established. In these cases, a fair implementation of user information and choice is necessary. Otherwise it is questionable whether a solution can be lawful.

4 Identity-related application scenarios and "data protection by default"

In this section, three examples for identity-related applications and potential defaults are discussed: social network sites, user tracking on the web and user-controlled identity management systems.

4.1 Social network sites

Although the discussion on "data protection by default" is much older, with social network sites it became apparent to huge parts of the society how important some privacy features are and what may happen if private information is widely distributed. One example is the problem with Facebook parties where users have accidentally invited thousands of members of the network instead of their small group of real friends. As already written in Section 2, the proposed European Data Protection Regulation explicitly demands mechanisms that prevent by default that personal data are made accessible to an indefinite number of individuals. [2]

Various research teams have investigated the value of privacy settings in social networks such as Facebook, e.g. [19], [20] and [21]. They found that, in large part, the privacy settings didn't match the users' expectations who typically expected a higher degree of privacy and less visibility of their personal data to others.

The understanding of privacy settings could be improved by an appropriate choice of words. For instance, a Facebook "friend" is not always a friend, and when it comes to friends of friends, this may sound nice and still quite intimate, but there is no reliable estimation of users who belongs to this category. For research purposes in [20], the Facebook category "everyone" for configuring the accessibility was renamed to "stranger". By this, the scope of potential access can be better expressed.

The question of "data protection by default" in practice for social network sites has been tackled by several researchers. In the work of [22], "privacy by design" and "privacy by default" have been analyzed separately. Whereas, among others, the aspect of allowing anonymous or pseudonymous use in social networks is considered a "privacy by design" requirement, the following collection of recommendations and considerations are categorized as "privacy by default" [22]:

- In the default setting, only the basic functionalities should be provided, i.e. only those personal data should be collected and used that are necessary for employing a

basic service as expected by the users. This also enables users to become familiar with the system.

- Additional privacy-related functionality needs explicit consent by users. For instance, external search engines should not be able to find a user or to access her data unless she opts in. The biometric analysis of photos would need explicit information of the data subject and her consent.
- The default setting for the visibility of profile or status data should be limited to the user's circle of close friends. There might be an exception for social networks that are dedicated to exchanging business contacts.
- If minors are member of the social network, the default settings have to be especially strict.
- Even with strict default settings a usage of the service should be possible. Otherwise there is a risk that users activate everything they can to overcome the limitations of the default settings.
- The provider has to inform the users about defaults and options in a comprehensible way in the registration process. They should be able to conveniently access and check their setting. The information should be well-arranged and easy to understand. Settings should be changeable at any time with effect for the future.

It should go without saying that personal data of non-members of a social network should not be collected unless they have given consent.

4.2 User tracking on the web

As soon as commercial sites became part of the World Wide Web, the tracking of users started – based on analysis of IP addresses, the referrer information or other browser chatter and cookies of different kinds. This information is being used especially for marketing research and for adjusting online advertisement according to the usage profile of the web surfers (behavioral targeting). Not always the data are matched to individual users, but at least the collected raw data has to be considered personal data. Most web browsers offer some possibilities for configuration, and several users install plug-ins that help them filtering tracking functions or advertisements. Still, the data collection by many web sites, directly or via third parties, doesn't comply with the requirements set out in the European e-Privacy Directive [23] or Member State's law.

Since 2007, consumer organizations in the U.S. have uttered the need for some "Do Not Track" solutions. In this situation, the World Wide Web Consortium took up a proposal of a "Do Not Track" (DNT) header that could be integrated in web browsers. Three different values of DNT are possible: "1" for "opt-out", meaning that the user does not want to be tracked; "0" for "opt-in", meaning that user consents to being tracked; and "null" (no header sent) if the user has not expressed a preference [24].

When Microsoft announced that their Internet Explorer 10 would be rolled out with default setting "1" (i.e. no tracking), several stakeholders in the U.S. regarded that as an affront since Microsoft, and not the user, would be exercising choice on the browser signal. They threatened to ignore all "no tracking" values sent from Internet

Explorers because these settings would represent a choice made by a company instead of the user herself.

However, the European Commission has clarified that "it is not the Commission's understanding that user agents' factory or default setting necessarily determine or distort owner choice. The specification need not therefore seek to determine the factory setting and should not do so, because to intervene on this point could distort the market. [...] the standard should foresee that at the install or first use of the browser the owner should be informed of the importance of their DNT choice, told of the default setting and prompted or allowed to change that setting." [25] Note that the Commission's statement does not judge on which default the factory setting should be preferred – this is left to the discretion of the browser producers.

This fight over the default setting for behavioral advertizing has an economic background. Even when surveys have shown that the majority of U.S. users as well as European users don't want to be tracked, the huge advertising industry strongly opposes the idea of a non-tracking default. It challenges the business model of offering services "for free" in exchange for collecting and analyzing personal data for individually targeted advertisements. So it may boil down to the question who will pay for web services and what privacy-respecting business models may work.

4.3 User-controlled managing of one's identities

User-controlled identity management systems assist and empower users to manage their own partial identities in their digital lives as well as their privacy [26]. They act as gateways and guardians between the user and her communication partners. It is not easy to define the right defaults in such concepts, because active privacy management by the users themselves require their understanding and control while the "data protection by default" principle mainly addresses those users who are not aware of the risks and are not willing or able to configure their system according to their needs. Of course, user-controlled identity management systems would have to inform and train users, but should not generally follow a too paternalistic approach which may be the case when deciding automatically on behalf of the users.

Still, a few guidelines can be given here, too:

- When user-controlled identity management systems are employed for achieving unlinkability between different partial identities, this has to be supported throughout all network layers: For instance, if linkable device IDs, IP addresses or browser chatter are communicated, the protection against linkage that private credentials can offer is void. Also, additional data hidden in files may jeopardize the protection. So metadata in documents or photos should not be disclosed to others unless explicitly chosen by the user. Note that this setting relies on additional privacy-by-design functionality.
- Naturally, all communication should be encrypted by default. Further, the storage of personal data under control of the user herself should be done in a highly secure and trustworthy area to protect unauthorized access.

- As design feature, warnings should be displayed by default if the personal data are to leave the area where the legal data protection framework relevant to the user (e.g. the European Economic Area for European citizens) can be enforced. This may be extended in cases of security or data protection breaches.
- By default, each new contact would mean to create and use a new pseudonym (representing another partial identity) if not stated otherwise. For existing contacts, a re-use of the already established pseudonym should be the default unless the user demands a new one. Note that this violates the rule of maximizing unlinkability for best privacy protection due to presumed functionality requirements: In user-controlled identity management systems, it should be the (changeable) default to enable longer lasting relationships with a communication partner instead of being limited to an anonymous use or one-time contacts.
- Only those attribute values that are necessary for the purpose should be released. The identity management system cannot decide on its own which attributes are needed. So here a fully automatic transfer of personal data without explicit and informed user consent is not advised. However, this process may be supported by certificates that communication partners (the "relying parties") can get from a trusted party after having assessed the necessity for the attributes for the specified purpose. For the German eID card, this is done to allow selective disclosure of attributes such as information about the age or the domicile, and to distinguish between usage under pseudonym or by giving the real name [27].

For attribute-based credentials that provide a more general solution on possible attributes that may be selectively disclosed meaningful and privacy-friendly defaults still have to be elaborated [28]. Also, the integration of additional parties that take part in the issuing or revoking process or may be relevant if an investigation is needed has to be considered when discussing privacy by default.

5 Conclusion

The principle "data protection by default" is part of the "privacy by design" approach. Although both "data protection by default" and "by design" have been incorporated as a legal requirement in the proposed European Data Protection Regulation [2], they are still not well defined. The Draft Report of the European Parliament on the Regulation [10] provides some clarification. But even this improved version of a legal proposal does not answer all questions for an application in practice.

Looking at various interpretations of the "data protection by default" principle, we conclude that two major types of configuration should be distinguished: the introduction of functionality with additional purposes on top of the basic system, and the setting of different options for components within the core application context. Whereas all additional functionality, that is not needed for the original purpose but can involve privacy risks, should be denied by default, the form of the preconfigured setting for mandatory functionality is not always clear when different options exist. However, such situations often require the user's awareness of the data processing and related risks so that a seamless interaction is not advised anyway. It is recommended that

users get the necessary information to compare settings regarding privacy risks and other relevant properties such as costs or required functionality. In many cases, a fully automatic decision on which defaults are the best for privacy cannot work since there is no overall accepted privacy metrics. Also, even privacy-aware users may have different preferences. In some cases localized defaults should be preferred over global settings, e.g. if the jurisdiction of processors plays a role. For those who don't want to delve into tailoring their settings, configuration providers can step in and offer meaningful defaults fitting various user groups.

An open question is whether "data protection by default" should try to maximize the privacy level when other kinds of data processing are privileged in data protection law. This is especially important for pseudonymous data processing that can massively reduce the risks to privacy in comparison to working with personal data on the basis of consent. Here "data protection by default" may mean "legally compliant by default" instead of "maximum privacy". In these cases, transparency on the defaults and ways for users to change them are essential.

Note that it is not sufficient to have good default settings if users are later on being tricked into releasing data or activating services. Experiments have shown that already the way in which individuals are asked for a decision concerning their privacy might influence their choice [29] – such psychological effects have to be further investigated. Supervisory authorities should demand neutral and fair information of users – otherwise a given consent might not be regarded as valid.

Whereas the default settings in the presented scenarios are important, but usually can be changed with some effort by the users, the choice of "data protection by default" becomes even more crucial when the personal computer as interface for looking at settings and changing them vanishes. With tablet computers and mobile phones, the convenience for reconfiguring the system already decreases. Similarly, Smart TVs that are based on web protocols appear to have similar privacy risks as browsing the Internet, but less configuration possibilities. Finally, for ubiquitous computing only few proposals exist on how "privacy by default" could be implemented [30].

All in all, the discussion on defaults should not promote that users lack necessary information and simply rely on the assumption that the best choice for them has been made already. This would not reduce, but rather increase the vulnerability of individuals' privacy.

Acknowledgments. I am grateful for the support of Jozef Vyskoč and Simone Fischer-Hübner throughout various versions of this text.

References

1. 32nd International Conference of Data Protection and Privacy Commissioners: Privacy by Design Resolution. Proposed by A. Cavoukian, approved in October 2010, Jerusalem, Israel, http://www.ipc.on.ca/site_documents/pbd-resolution.pdf (2010)
2. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and

on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final, Brussels, 25.01.2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (2012)
3. Hansen, M., Probst, T.: Datenschutzgütesiegel aus technischer Sicht: Bewertungskriterien des schleswig-holsteinischen Datenschutzgütesiegels. In: Bäumler, H., von Mutius, A. (eds.) Datenschutz als Wettbewerbsvorteil – Privacy sells: Mit modernen Datenschutz-komponenten Erfolg beim Kunden, pp. 163–179. Vieweg, Wiesbaden (2002)
4. European Privacy Seal, https://www.european-privacy-seal.eu/
5. Nielsen, J.: The Power of Defaults. Jakob Nielsen's Alertbox, September 26, 2005, http://www.useit.com/alertbox/defaults.html (2005)
6. Kesan, J.P., Shah, R.C.: Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics. U Illinois Law & Economics Research Paper No. LE06-012. Notre Dame Law Review, vol. 82, 583–634 (2006)
7. Bureau Européen des Unions de Consommateurs (BEUC): EU General Data Protection Framework – BEUC answer to the consultation. December 31, 2009, http://www.beuc.org/custom/2010-00021-01-E.pdf (2009)
8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031–0050 (1995)
9. European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the data protection reform package. March 7, 2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf (2012)
10. Albrecht, J.P. (Rapporteur): Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, 17.12.2012, http://www.europarl.europa.eu/sides/getDoc.do?language=EN&reference=PE501.927 (2012)
11. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles. August 2009, revised January 2011, http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf (2011)
12. Reding, V.: Your data, your rights: Safeguarding your privacy in a connected world. Privacy Platform "The Review of the EU Data Protection Framework", Brussels, March 16, 2011, Reference: SPEECH/11/183, http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm (2011)
13. Altheim, M.: The Review of the EU Data Protection Framework v. The State of Online Consumer Privacy in the US. Blog entry, March 17, 2011 http://ediscoverymap.com/2011/03/the-review-of-the-eu-data-protection-framework-v-the-state-of-online-consumer-privacy-in-the-us/ (2011)
14. Scarfone, K., Hoffman, P.: Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. Special Publication 800-41, Revision 1, September 2009, http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf (2009)
15. Lipner, S., Howard, M.: The Trustworthy Computing Security Development Lifecycle. MSDN, March 2005, Security Engineering and Communications, Security Business and Technology Unit, Microsoft Corporation, http://msdn.microsoft.com/en-us/library/ms995349.aspx (2005)

16. Soghoian, C.: Not an option: time for companies to embrace security by default. Ars Technica, August 9, 2011, http://arstechnica.com/tech-policy/2011/08/not-an-option-time-for-companies-to-embrace-security-by-default/ (2011)
17. Iachello, G., Hong, J.: End-User Privacy in Human-Computer Interaction. Found. Trends Hum.-Comput. Interact., vol. 1, no. 1, pp. 1–137. Now Publishers Inc., Hanover, MA (2007)
18. Microsoft: Privacy by Default. March 2012, http://download.microsoft.com/download/B/8/2/B8282D75-433C-4B7E-B0A0-FFA413E20060/privacy_by_default.pdf (2012)
19. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing Facebook Privacy Settings: User Expectations vs. Reality. In: IMC '11 Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pp. 61–70. ACM, New York, NY (2011)
20. Madejski, M., Johnson, M., Bellovin, S.M.: The Failure of Online Social Network Privacy Settings. Tech Report CUCS-010-11, Columbia University (2011)
21. Rubinstein, I.S., Good, N.: Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents". New York University Public Law and Legal Theory Working Papers, Paper 347, http://lsr.nellco.org/nyu_plltwp/347 (2012)
22. Niemann, F., Scholz, P.: Privacy by Design und Privacy by Default – Wege zu einem funktionierenden Datenschutz in Sozialen Netzwerken. In: Peters, F., Kersten, H., Wolfenstetter, K.-D. (eds.) Innovativer Datenschutz, pp. 109–145. Duncker & Humblot, Berlin (2012)
23. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037–0047, amended in 2009 by the Directive 2009/136/EC of 25 November 2009 (2009)
24. Fielding, R.T., Singer, D. (eds.): Tracking Preference Expression (DNT). W3C Working Draft 02 October 2012. http://www.w3.org/TR/tracking-dnt/ (2012)
25. European Commission, Director-General (Robert Madelin): Letter to World Wide Web Consortium Tracking Protection Working Group. Ref. Ares(2012)743354, June 21, 2012, http://lists.w3.org/Archives/Public/public-tracking/2012Jun/att-0604/Letter_to_W3C_Tracking_Protection_Working_Group.210612.pdf (2012)
26. Hansen, M.: User-controlled identity management: the key to the future of privacy? In: International Journal of Intellectual Property Management (IJIPM), vol. 2, no. 4, pp. 325–344. Inderscience Publishers, Olney (2008)
27. Zwingelberg, H., Hansen, M.: Privacy Protection Goals and Their Implications for eID Systems. In: Jan Camenisch et al. (eds.) Privacy and Identity 2011, IFIP AICT 375, pp. 245–260. IFIP International Federation for Information Processing (2012)
28. ABC4Trust – Attribute-based Credentials for Trust, FP7 ICT Integrated Project, https://abc4trust.eu/
29. Acquisti, A., John, L., Loewenstein, G.: What is privacy worth? In: Workshop on Information Systems and Economics (WISE), http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf (2009)
30. Schmitt, L.: Privacy as default. Privacy by default! Konzept für Privatsphäre im Ubiquitous Computing. Diploma Thesis, Köln International School of Design, June 2006, http://lutzschmitt.com/pub/Lutz_Schmitt-Privacy_as_default_Privacy_by_default.pdf (2006)