Data Protection by Design and by Default à la European General Data Protection Regulation

Marit Hansen(✉)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
marit.hansen@datenschutzzentrum.de

Abstract. The European data protection reform has resulted in a new regulation that will be effective from May 2018. This so-called General Data Protection Regulation contains specific provisions on data protection by design and on data protection by default. After briefly discussing related approaches such as "privacy by design", we will elaborate how these provisions can be interpreted and sketch the potential impact on data processing in Europe and possibly beyond.

Keywords: Data protection · European General Data Protection Regulation · Data protection by design · Data protection by default · Privacy · Privacy by design · Privacy by default

1 Introduction

For decades, the concept of "privacy by design" is being discussed and recommended by Data Protection and Privacy Commissioners [1]. In short, "privacy by design" means a design of systems where privacy requirements have been considered and appropriate measures to fulfil these requirements have been implemented – resulting in built-in privacy. "Privacy by design" should be applied in all phases of system development. As a rule, this method is superior to an attempt of subsequently adding some privacy features to a running system: Refraining from giving thought to privacy requirements in the design process usually yields systems that determine the data processing to a large extent with the effect that specifically data minimisation requirements won't be easy to implement in the best possible way later on. Also, tailoring an existing system to privacy needs that were ignored before may be a cumbersome and expensive task, if possible at all.

However, today's reality of system design doesn't reflect that demand. "Privacy by design" is the exception and not the rule. The monetary incentives for developers to adhere to this paradigm are few, and by now there are no perceptible sanctions for the responsible entities (data controllers or data processors) using systems without built-in privacy as long as the data processing is sufficiently legally compliant otherwise [2]. In this situation, producers of systems may regard each requirement that should be considered in addition to the bare functionality of their system as overly complex and reject any delay in the time to market. Even the often demanded "security by design" paradigm is by no means normal practice so that adversaries can frequently take advantage of vulnerabilities in IT systems.

A. Lehmann et al. (Eds.): Privacy and Identity 2016, IFIP AICT 498, pp. 27–38, 2016.
DOI: 10.1007/978-3-319-55783-0_3

These observations were considered by the European Union lawmakers when debating the data protection reform in the recent years. One important outcome is the General Data Protection Regulation (GDPR) [3] that demands not only that appropriate security measures are implemented by controllers processing personal data, but also "data protection by design and by default" (Article 25 GDPR). The GDPR, and specifically the provisions on data protection by design and by default, may become a game changer with respect to guaranteeing the rights and freedoms of human beings, including the right to privacy. Therefore this text will provide a deeper look into the General Data Protection Regulation and its demands for designing systems according to data protection requirements.

This text is organised as follows: Sect. 2 sketches important properties of the European General Data Protection Regulation resulting from the European data protection reform initiative. The related concept of "privacy by design" is introduced in Sect. 3 which provides brief information on the history and on definitions. Sections 4 and 5 dig into the legal obligations concerning data protection by design and data protection by default, respectively. Finally, Sect. 6 summarises the findings and gives a conclusion.

2 The General Data Protection Regulation

In 1995 the European Union adopted the Data Protection Directive 95/46/EC [4] which then had to be implemented by each member state. Although the Data Protection Directive aimed at a harmonised and modern data protection regime throughout Europe, this objective was not fully achieved due to differences in the various national implementations. In 2016, more than 20 years later, the successor of the Data Protection Directive was adopted after several years of discussion and negotiation: the General Data Protection Regulation [3]. Lessons learnt from the experience of the former data protection regime were considered and, again, the goals of harmonisation and modernisation were pursued. The GDPR will become effective May 25, 2018. Its direct applicability in all member states will help unifying the data protection level. However, about 70 opening clauses – some mandatory, some optional – provide means for own national requirements and thereby deviation from a joint strategy across the member states [5].

The GDPR cannot be a panacea for data protection at its best: Not everything in the GDPR is brandnew, and the 99 Articles leave room for interpretation. The chosen level of abstraction in the legal text may at first seem to lack support for those who have to comply with the GDPR. But this is an intended feature rather than a bug: Abstract rules need to be substantiated in a way that is appropriate with respect to the ever-changing risk to rights and freedoms of natural persons and accepted among the European data protection commissioners as supervisory authorities. So the GDPR defines a process for achieving consistency in the interpretation of the legal obligations concerning cross-border cases. By this, the GDPR may be future-proof for several years or even multiple decades – unlike its predecessor. However, steady negotiation on the substantiation of abstract rules is time-consuming and may be influenced by lobbyists who don't share the goal of optimal data protection.

It has to be noted that the GDPR does not only address European data controllers, but is designed to guarantee data protection in the entire European market. The market location principle laid down in Article 3 GDPR addresses organisations that offer goods or services to people in the EU or monitor their behaviour, even if the organisations are not established in the territory of the European Union. In particular those non-EU companies dominating the digital market shall comply with the data protection requirements in the GDPR.

Whether the GDPR will provide the proper instruments for achieving data protection cannot be predicted at this early stage. However, clearly the European member states have a joint starting point to take it from there. This is true for all instruments described in the GDPR, e.g. data protection by design, data protection by default, data protection impact assessment, codes of conduct, certifications, sanctions, or the involvement of courts.

In the following, we will focus on design issues demanded by the GDPR. This is in line with the statement in Recital 4 of the GDPR: *"The processing of personal data should be designed to serve mankind."*

3 Privacy by Design

Building in privacy – or, to use the same wording as the GDPR: data protection[1] – has been proposed by various stakeholders for several decades. In addition to cryptographic functionalities to achieve confidentiality or integrity, concepts for privacy technologies were proposed for more than 30 years (e.g. [6]). Since the mid-1990ies the term "Privacy-Enhancing Technologies (PETs)" became known in the Data Protection Commissioners' community [7] and was taken up by the European Commission:

> *"The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them."* [8]

When the former Ontario Privacy Commissioner Ann Cavoukian promoted the concept of "Privacy by Design" [9] and described seven foundational principles [10], she extended the scope by addressing IT systems, accountable business practices, and physical design and networked infrastructure. It is important to understand that system

[1] It has to be stressed that "privacy" and "data protection" denote different, but related concepts, and there is not one single definition each. Usually the meaning of "privacy" points to the rights of an individual and is associated with self-defence against intrusion. "Data protection", as coined in European data protection law, addresses primarily organisations that have to make sure that the rights of the individuals are not infringed. Note that Article 8 of the European Convention on Human Rights and similarly Article 7 of the Charter of Fundamental Rights of the European Union provide a right to privacy: "Right to respect for private and family life". In addition, Article 8 of the Charter focuses on data protection: "Protection of personal data". For the purpose of this text it is not necessary to precisely define the boundaries because the exact privacy and/or data protection requirements to be built in would differ for various cases and cannot be elaborated in detail at this point.

design must not be limited to adding a few PET modules, but needs a more comprehensive approach that encompasses in particular hardware and software, interfaces, organisational processes, and business models.

Engineers expect a more detailed operationalisation and specification for the task of building in privacy requirements. Different proposals have been made in the last few years to support engineering privacy (e.g., [11–15]), and there are studies such as [16] that summarise the current status of research and point out obstacles. However, today's IT development environments refrain from making developers aware of privacy requirements.

From the legal perspective, some researchers argued that the European Data Protection Directive 95/46/EC already contained the requirement for privacy by design: *"The incorporation of PETs into strategies for privacy receives some encouragement from Article 17 of the Directive, which requires data controllers to implement 'appropriate technical and organisational measures' to protect personal data, especially in network transmissions. Recital 46, which augments the meaning of Article 17, highlights the requirement that these measures should be taken 'both at the time of the design of the processing system and at the time of the processing itself', thus indicating that security cannot simply be bolted onto data systems, but must be built into them."* [17] However, this demand for "appropriate technical and organisational measures" primarily calls for "security by design" and not so much for "data protection by design", although a few member states incorporated legal provisions for anonymisation or other data minimising functionality [17, 18].

For instance, the German Federal Data Protection demands in § 3a concerning data minimisation: *"Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. […]"* [18] All the same, this legal provision has proven ineffective since no fines can be imposed in case the controller ignores that obligation.

This is different with Article 25 GDPR "Data protection by design and by default" where the supervisory authority has to ensure the imposition of administrative fines in case the obligations of the controller or the processor pursuant to Article 25 have been infringed (Article 83 (4) lit. a)). The administrative fine has to be effective, proportionate and dissuasive (Article 83 (1)) and may go up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

As a rule, all European language versions of the GDPR are equally valid. However, there is a noteworthy difference in the title of Article 25, as the following excerpt shows:

- [EN] Article 25: Data protection by design and by default
- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen
- [SV] Artikel 25: Inbyggt dataskydd och dataskydd som standard
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Most of the languages reflect the "design" idea, the Swedish translation focuses on the "built-in" part. Only the German version adds "Technik" (technology) in the title of Article 25 which may be misleading because – as stated before – privacy by design must not be reduced to technology in a narrow sense, but has to reach out to entire systems and services. Probably this wording has been used in the German version of the GDPR in association with the long-standing concept "Datenschutz durch Technik" (literal translation: "data protection by technology") which was introduced in the mid-1990ies to denote the work on Privacy-Enhancing Technologies [7] and privacy by design. Recital 78 of the German GDPR even mentions "Datenschutz durch Technik", but adds the translation "data protection by design".

Article 25 GDPR consists of three paragraphs: The first paragraph deals with data protection by design (cf. Sect. 4), the second tackles data protection by default (cf. Sect. 5), and the third paragraph, which won't be further discussed in this text, adds a remark on the relation to certification.

4 Data Protection by Design

Article 25 (1) GDPR reads as follows:

> *"(1) Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."*

For a better understanding, this long sentence is disassembled and put into context:

Who shall take an action?

- The controller.
- There are also indirect effects on potential data processors, acting on behalf of the controller, as well as on producers of systems because the controller would have to choose products, services and applications in such a manner that the requirements of the GDPR are met and ensure the protection of the rights of the data subjects (cf. Article 28).

What is the objective?

- Meeting the requirements of the GDPR and protecting the rights of the persons concerned ("data subjects").
- This means in particular to implement the data protection principles that are laid down in Article 5 of the GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability.

What has to be done?

- Implementing appropriate technical and organisational measures in an effective manner.

- Integrating the necessary safeguards into the processing.

How should it be done?

- Both at the time of the determination of the means for processing and at the time of the processing itself.
- In an effective manner.

Which conditions occur?

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purposes of processing.
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

The conditions are of utmost interest because they can constitute both an upper and lower bound for the actions to be taken. The data controller needs to employ these conditions to justify all decisions concerning the implementation of measures: How were the measures chosen, why were better measures omitted? In the beginning, the given conditions will probably function mainly as a limitation of what the controller has to do for data protection by design. But at least the justification has to be done and should be documented so that supervisory authorities are able to check whether the grounds for not implementing better measures are plausible.

One limiting factor will be the state of the art: In the last years the state of research in "privacy by design" has made good progress, but the transition to state-of-the-art measures is not an easy task and cannot be taken for granted. Concerning Article 25 GDPR, it will be debated in many cases whether a measure belongs to the category "state-of-the-art". However, for deciding on "state of the art" it is not sufficient to determine solely the readiness of a measure such as a Privacy-Enhancing Technologies, but also the quality for improving or ensuring data protection has to be taken into account. The metrics for such a combined maturity assessment and the evaluation procedure are by no means trivial. Instead they require expert knowledge when trust assumptions, potential side effects, or usability issues have to be considered [19].

In the realm of security, the category "state of the art" should already be known from Article 17 (1) of the European Data Protection Directive 95/46/EC:

> *"Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data […]. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."* [4]

Similarly, Article 32 demands the usage of appropriate state-of-the-art security measures. Judging from many discussions after the adoption of the GDPR, the exact properties of when to consider a security measure state of the art have not been fully defined, although this requirement has been laid down in European data protection law at least since 1995.

Likewise, surprisingly little information is available on state-of-the-art measures concerning privacy by design. Determining good and best practices of concepts and products as well as agreeing on their classification as state of the art will certainly become a task for the supervisory authorities. Anyhow, Article 24 on the responsibility of the

controller clarifies that the controller has to implement "appropriate technical and organisational measures to ensure and to be able to demonstrate" compliance with the GDPR. The factors "state of the art" and "cost of implementation" are left out in that provision.

Article 25 (1) GDPR and the accompanying Recital 78 mention a few examples (explicitly stated: "inter alia") for measures that may be appropriate:

> *"[…] minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features."* (Recital 78 GDPR)

Thereby not only privacy-enhancing technologies, but also transparency-enhancing technologies (TETs) are addressed. Further, this recital acknowledges that the controller may have to advance the security features, e.g. in the case of sensitive data. "One size fits all" wouldn't live up the expectations of the GDPR. The improvement of security features is also demanded when vulnerabilities in the provided functionality are becoming known. This requires an ongoing risk monitoring in a data protection management system.

What is more, Recital 78 addresses producers of products, services and applications who "should be encouraged to take into account the right to data protection when developing and designing such products, services and applications" so that controllers "are able to fulfil their data protection obligations". Recital 78 gives one example that can really encourage producers to invest in privacy by design: "The principles of data protection by design and by default should also be taken into consideration in the context of public tenders." Thus, procurement processes should from now on incorporate built-in data protection.

5 Data Protection by Default

The text of Article 25 (2) GDPR reads as follows:

> *"(2) The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."*

The nature of the second paragraph of Article 25 GDPR is totally different from the first paragraph since it omits the explicit mentioning of limiting factors. Still, the word "appropriate" gives room for interpretation of which measures are suitable and right for the purpose.

Again, the controller is responsible for implementing technical and organisational measures. In the first sentence, the data minimisation principle (cf. Article 5 (1) lit. c) GDPR) and the purpose limitation principle (cf. Article 5 (1) lit. c) GDPR) are repeated. The insertion of "by default" addresses the standard configuration of a data processing system.

The second sentence specifies that not only the amount of the data collected, but also the extent of their processing, the storage duration and the accessibility of the personal data are affected. Thereby the standard configuration should prevent that personal data which are not strictly necessary for the purpose are processed at all (e.g. by limiting the personal data that is asked for), that they are processed only to the extent as necessary for the purpose (e.g. by restricting the possible processing steps or by using data minimisation measures such as anonymisation or pseudonymisation functionalities), that they are erased as early as possible regarding the purpose (e.g. by automatic erasure measures), and that their accessibility is limited as much and as soon as the purpose allows (e.g. by access control mechanisms, by carefully choosing the storage location, or by encrypting the data).

The third sentence gives an example that relates to Internet publications or social networks: that, by default, personal data must not be made accessible to an indefinite number of people.

The notion of "default" incorporates the possibility to change the default setting. The last sentence of Article 25 (2) GDPR it clarifies that "the individual's intervention" may allow changing the configuration. The default setting would be the initial configuration which can be changed by the data subject to allow that more data are processed, that other processing steps are allowed, that the data can be stored for a longer time, and that they may be accessible to other parties as well. Typical cases where this may be desired by a data subject comprise sharing information on the web or in a social network, creating accounts as returning customers so that information on their mail address or on payment methods is stored for the next visit, or providing personal data for long-term personalised consumer experiences.

The GDPR interpretation of "data protection by default" differs from previous ideas in the privacy-by-design context where Cavoukian demanded:

> *"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."* [10]

This requirement sounds promising, but if "intact privacy" means that no personal data are processed at all or that there is a guarantee of no risk for the individual's privacy, many real cases with lawful and legitimate purposes would not work. As soon as the individual chooses to make use of a product or a service, this may require processing of personal data and thereby wouldn't necessarily considered as leaving the individual's privacy intact. Perhaps this notion rather addresses the individual's horizon of expectation: For users of a product or service it should be clear which personal data are needed for the purpose (e.g. basing on informed consent), and all additional data processing should be prevented unless the user intervenes and changes the setting. However, the product or service should not create the false impression that the functionality can be offered when the user sticks to a default of no-disclosure of personal data, e.g. when a governmental service will require specific attributes of the citizen for the payment of social benefits. But this will be probably meet the expectations of the user.

A more elaborate view on data protection by default was given by the European Data Protection Supervisor when commenting a previous version of Article 25 GDPR:

"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." [20]

Here the aim is not to leave privacy intact, but to – at least initially – limit privacy intrusive features. The statement stresses that the guideline for deciding what is necessary should be the simple use of a product or service. This also means that the individual should be able to use a product or service even if disclosing or storing more personal data may mean extended functionalities or a different user experience.

Today only very few guidelines on "data protection by default" exist (one example is the workflow given in [21]). So it is difficult both for data controllers and for supervisory authorities to decide on an appropriate default setting. In any case it will have to be determined in a first step which parts are hardwired without the possibility for a change (which relates back to "data protection by design" and built-in data protection) and which parts are configurable. For the configurable part it has to be figured out when and which pre-settings are reasonable for which user groups (e.g. different settings for children and adults, or different settings for EU residents and non-EU residents when it comes to storage location) and when the configuration should be better done in an interaction with the user when installing the system.

Also it has to be given thought to usable ways of changing the configuration later on in an informed manner and without giving up all protection at once. It shouldn't be the case that the solution with the data protection default setting is barely usable, but one click away is the full version that entails no protection at all (which may infringe Article 7 (4) GDPR on freely given consent). The known challenge how to prevent that people get overwhelmed or tired from the configuration possibilities may become even harder if data controllers – not being enthusiastic about data protection by default – put the blame on data protection regulators. Thus, a static "take it or leave it" default is probably not the best solution. Instead, taking the pre-configured default as a starting point, users should be supported in choosing the best fitting configuration (see e.g. [22]), or they could even profit from the approach of "on the fly" privacy management for adapting and organising their own privacy preferences [23].

Finally, data protection by default can ruffle the feathers of established Internet business models. For instance, according to Article 25 (2) GDPR user tracking on the basis of personal data (including machine identifiers) would have to be deactivated as a standard setting. This may affect the tradition of "free" services where Internet resources are paid by personal data.

6 Conclusion

The European General Data Protection Regulation contains legal provisions on data protection by design and by default. This obligation addresses data controllers who have to consider building in data protection functionality in their systems. In addition, it holds the potential of affecting the currently not well developed market in privacy and data

protection systems and services. The GDPR offers the opportunity for bridging the gap between research and practice in the field of privacy and data protection.

Although not really new, both data protection by design and data protection by default are powerful mechanisms and may become a game changer if taken seriously by controllers, processors, producers, and supervisory authorities. However, employing these principles is a challenging task for all stakeholders involved and requires in-depth knowledge of research concepts and state-of-the-art implementations. So as not to negate the leverage from the GDPR, researchers, practitioners, and supervisory authorities should collaborate and propose suitable best practice approaches. It should be made difficult to ignore the laid down rules or to shirk responsibilities and obligations regarding the system design requirements. Nevertheless a broad use of data protection design methods and measures has to rely on thoroughly discussed, tested, and workable solutions. Further, infrastructures should not only realise data protection by design themselves, but also promote and support measures built on top or employing functionality offered. This will be primarily a task for the member states or the European Union.

Although the GDPR becomes effective only in May 2018, the interdisciplinary work of computer scientists, developers, lawyers, psychologists, economists etc. should begin much earlier [10]. The lack of a holistic approach for engineering and promoting privacy technologies is certainly one reason for the unsatisfactory status of their maturity and their market availability. Even good approaches can fail if the ecosystem for their usage is not sufficiently considered, business models are missing, users don't understand their value or perceive losses in comfort compared with the not-so-privacy-friendly solutions they are familiar with (see e.g. [24]). Interdisciplinary work takes time and does not happen automatically – it requires a common understanding of the problem space as well as openness for underlying incentives and values of other disciplines [25]. This includes the supervisory authorities which will have to evolve to live up the tasks they have been imposed by the GDPR and to actively seize opportunities for improving the protection of rights and freedoms of all individuals.

If recommendations and ready-to-use concepts are developed and published soon enough, this facilitates data controllers to prove their compliance with the regulation from day one and, at best, set an example of international relevance regarding data protection by design and by default. It is noteworthy that the GDPR is designed to have an influence beyond Europe because it strives to protect the personal data of EU residents even outside the European Union and obliges also non-EU controllers processing personal data in Europe. What is more, whenever successful solutions are being developed, they may be demanded by all people inside and outside Europe interested in protecting their right to privacy and may be expected especially from globally acting companies. Data protection by design and by default is of particular relevance in a world that relies increasingly on digitisation and that has to defend the rights and freedoms of individuals against attacks from powerful organisations.

Acknowledgements. Work relating to this text is partially funded by the German Ministry of Education and Research within the project "Privacy-Forum – Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt (Forum Privacy and Self-determined Life in the Digital World)". For more information see: https://www.forum-privatheit.de/.

References

1. 32nd International Conference of Data Protection and Privacy Commissioners: Privacy by Design Resolution, Jerusalem, Israel, 27–29 October 2010. http://www.ipc.on.ca/site_documents/pbd-resolution.pdf
2. Roussopoulos, M., Beslay, L., Bowden, C., Finocchiaro, G., Hansen, M., Langheinrich, M., Le Grand, G., Tsakona, K.: Technology-induced challenges in privacy & data protection in Europe. Technical report. ENISA Ad Hoc Working Group on Privacy & Technology (2008). https://www.enisa.europa.eu/publications/technology-induced-challenges-in-privacy-data-protection-in-europe
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 04.05.2016, pp. 1–88 (2016)
4. 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. OJ L 281, 23.11.1995, pp. 0031–0050 (1995)
5. Roßnagel, A., Nebel, M.: Die neue Datenschutzgrundverordnung – Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet? Policy Paper, Privacy-Forum (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt) (2016). https://www.forum-privatheit.de/
6. Chaum, D.: Security without identification: transaction systems to make big brother obsolete. Commun. ACM **28**(10), 1030–1044 (1985)
7. Hes, R., Borking, J.J.: Privacy-enhancing technologies: the path to anonymity. Technical report. Registratiekamer (1995)
8. European Commission: Privacy Enhancing Technologies (PETs) – the existing legal framework. MEMO/07/159 (2007)
9. Cavoukian, A.: Privacy by Design, Take the Challenge. Information and Privacy Commissioner of Ontario, Toronto (2009)
10. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles (August 2009, revised January 2011)
11. Gürses, S., Troncoso, C., Díaz, C.: Engineering privacy by design. In: Computers, Privacy & Data Protection (2011)
12. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Eng. J. **16**(1), 3–32 (2011)
13. Hoepman, J.-H.: Privacy design strategies (extended abstract). In: Proceedings of SEC 2014, ICT Systems Security and Privacy Protection, pp. 446–459 (2014)
14. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: Proceedings of the 1st International Workshop on Privacy Engineering. IEEE (2015)
15. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (2016). https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf
16. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., Schiffner, S.: Privacy and Data Protection by Design – from policy to engineering. Technical report. ENISA (2015). https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design
17. Borking, J.J., Raab, C.D.: Laws, PETs and other technologies for privacy protection. J. Inf. Law Technol. (JILT) **1**(1), 1–14 (2001)

18. Bundesdatenschutzgesetz (BDSG). BGBl. I Nr. 3, 24.01.2003, Bonn, pp. 66–88 (2003)
19. Hansen, M., Hoepman, J.-H., Jensen, M.: Readiness analysis for the adoption and evolution of privacy enhancing technologies – methodology, pilot assessment, and continuity plan. Technical report. ENISA (2015). https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets
20. European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf
21. Hansen, M.: Data protection by default in identity-related applications. In: Fischer-Hübner, S., Leeuw, E., Mitchell, C. (eds.) IDMAN 2013. IFIP AICT, vol. 396, pp. 4–17. Springer, Heidelberg (2013). doi:10.1007/978-3-642-37282-7_2
22. Ravichandran, R., Benisch, M., Kelley, P.G., Sadeh, N.M.: Capturing social networking privacy preferences: can default policies help alleviate tradeoffs between expressiveness and user burden? In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 1–18. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03168-7_1
23. Angulo, J., Fischer-Hübner, S., Wästlund, E., Pulls, T.: Towards usable privacy policy display and management. Inf. Manag. Comput. Secur. **20**(1), 4–17 (2012)
24. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In: Cristofaro, E., Wright, M. (eds.) PETS 2013. LNCS, vol. 7981, pp. 245–264. Springer, Heidelberg (2013). doi:10.1007/978-3-642-39077-7_13
25. Tsormpatzoudi, P., Berendt, B., Coudert, F.: Privacy by design: from research and policy to practice – the challenge of multi-disciplinarity. In: Berendt, B., Engel, T., Ikonomou, D., Le Métayer, D., Schiffner, S. (eds.) APF 2015. LNCS, vol. 9484, pp. 199–212. Springer, Heidelberg (2016). doi:10.1007/978-3-319-31456-3_12