PRIPARE: A New Vision on Engineering Privacy and Security by Design

Nicolás Notario[1(✉)], Alberto Crespo[1], Antonio Kung[2], Inga Kroener[3], Daniel Le Métayer[4], Carmela Troncoso[5], José M. del Álamo[6], and Yod Samuel Martín[6]

[1] Atos Spain S.A., Madrid, Spain
{nicolas.notario,alberto.crespo}@atos.net
[2] Trialog, Paris, France
antonio.kung@trialog.com
[3] Trilateral, London, UK
inga.kroener@trilateralresearch.com
[4] Inria, Lyon, France
daniel.le-metayer@inria.fr
[5] Gradiant, Vigo, Pontevedra, Spain
ctroncoso@gradiant.org
[6] Universidad Politécnica de Madrid (UPM), Madrid, Spain
{jmdela,samuelm}@dit.upm.es

Abstract. The new EU Data Protection Directive (DPD), approved by the EU Parliament acknowledges the need of Data Protection by Design and by Default in order to protect the rights and freedoms of data subjects with regard to the processing of personal data. PRIPARE confronts the lack of a truly engineering approach for these concepts by providing a methodology that merges state-of-the-art approaches (e.g. Privacy Impact Assessment and Risk management) and complements them with new processes that cover the whole lifecycle of both, personal data and development of ICT systems.

Keywords: Privacy by design · Security by design · Methodology · Privacy

1 Introduction

The Universal Declaration of Human Rights declares in Article 12 that “No one shall be subjected to arbitrary interference with his privacy. … Everyone has the right to the protection of the law against such interference or attacks” [1]. Recent revelations of mass surveillance have put privacy at the forefront of political and societal debate and uncovered serious violations and lack of effective respect for this human right. As it is impossible to think of a violation of human rights at such scale in the “offline world” without international condemnation, the United Nations (UN) has reacted to these events in the “digital world” by adopting a resolution that affirms “that the same rights that people have offline must also be protected online, including the right to privacy” [2]. The same resolution also calls on countries “To review their procedures, practices and legislation regarding the surveillance of communications, their

F. Cleary and M. Felici (Eds.): CSP Forum 2014, CCIS 470, pp. 65–76, 2014.
DOI: 10.1007/978-3-319-12574-9_6

interception and collection of personal data including mass surveillance, interception and collection" [2].

In the EU, the current legislative process to approve the EU General Data Protection Regulation (GDPR) can be seen to be in line with this UN request and is aimed to effectively strengthen European citizens' privacy, in particular in the area of personal data protection. As reality demonstrates, a strong and consistent legal framework on its own is not sufficient to guarantee that stakeholders will correctly adopt adequate privacy practices. The Privacy by Design (PbD) concept has been around since the 90's. Cavoukian's 7 Foundational Principles articulation [3] of PbD is widely acknowledged by data protection commissioners world-wide, and there is growing evidence that this truly transformative approach has the potential to create far-reaching impact and benefits for citizens, government and business, as well as in several economic, industrial and ICT domains (e.g. health, energy, cloud, mobile/communications, Near Field Communication (NFC)/Radio Frequency IDentification (RFID), geolocation, big data/data analytics, surveillance and authentication technologies). While there is a unanimous consensus on the benefit of the principles in terms of privacy awareness, unfortunately there is still a lack of a systematic approach that would help businesses and organizations to include privacy-supportive processes and practices in their products and services. The new European GDPR, in its Article 23, states that controllers shall follow the data protection by design and by default principle, following the opinion of data protection authorities such as:

- The European Data Protection Supervisor (EDPS): Opinion of the EDPS on Promoting Trust in the Information Society by Fostering Data Protection and Privacy [4],
- The Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals [5].

Whenever it is approved, compliance with the new Regulation on Data Protection will further spark interest in the need to follow PbD principles and approach. Some industries particularly vulnerable to privacy risks have anticipated proactively developing tools that address privacy concerns (i.e. the RFID industry and the EU RFID Privacy Impact Assessment (PIA) [6]).

PRIPARE (www.pripare.eu) project has two important missions:

- To design and facilitate the application of a PbD and Security-by-Design (SbD) methodology (PRIPARE methodology) in the ICT research community in preparation for industry practice.
- To foster a risk management culture within organizations by preparing best practices material, supporting FP7 and Horizon 2020 research projects, providing educational material on approaches to risk management of privacy, and by identifying gaps and providing recommendations on Privacy and Security-by-Design (PSbD) practices.

The PRIPARE methodology will allow forging sustainable links between the different privacy stakeholders (regulators, educators, engineers and standardization organisms) in order to set the necessary common grounds on which to build trustworthy and privacy-respectful systems. Increasing levels of public trust in ICT systems will:

- Facilitate faster adoption of new services and technologies that feature high and tangible levels of privacy and security embedded into their design and provided by default;
- Increase the speed of innovation and creation of added value for a more competitive European ICT industry;
- Contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance.

In Sect. 2 we underscore the complexity involved in achieving a common understanding of privacy and security by design and what are the current approaches for addressing this complexity. In Sect. 3, we provide the rationale behind the need to agree on a common terminology for privacy among different stakeholders and approach followed for this in PRIPARE project. Section 4 outlines the identified security and privacy and security principles that will be embedded in the PRIPARE methodology. Section 5 presents an outline of the PSbD methodology which will address existing PSbD engineering problems, explaining (in Sect. 6) the relationship of PRIPARE's PSbD methodology with other existing methodologies. The paper concludes with some remarks and a draft of future work for PRIPARE methodology.

2 Taking Privacy by Design One Step Further

Very often privacy is (or seems to be) in tension with other requirements, and the design space of data minimization can be very wide, with different options providing different types of benefits and drawbacks. Therefore it is of prime importance to be able to make reasoned decisions and to be able to justify them. As far as privacy is concerned, these decisions must be based on a privacy risk analysis in which the privacy values at stake are clearly defined, as well as the sources of risks and their potential impact on these values. The result of this analysis should guide the choice of appropriate solutions (architecture and tools) and serve as justification for this choice. Sources like legislation, industry standards, and guidance produced by trade bodies, regulators, or other organizations working in their sector can be used to identify privacy and related risks that then can be minimized.

There is a strong and clear relationship between privacy and identity management. Identity management refers to the set of processes that administers the life cycle (collection, authentication, use, and deletion) of an identity, and the data linked to it, within an organization or system and across its boundaries. Identity management systems designed to follow privacy and security principles will provide their users with tools that allow them to manage their privacy in a reliable, trustable, and usable way. Failing to follow these principles can lead to flawed systems that pose serious privacy threats like identity theft or unintentional disclosure of personal data.

Identity management systems have evolved from silo-like approaches, where all the identity information is kept and used within a single organization, to federated, or network-centric, approaches where the underlying infrastructure enables a participating entity to share their users' personal data with others, e.g. by means of the OASIS (Organization for the Advancement of Structured Information Standards) Security Assertion Markup Language, Liberty's Identity Web Services Framework, or OpenSocial technologies, among others.

Several solutions have been proposed to develop a privacy-enhancing identity management infrastructure including the use of pseudonyms and attribute-based (or zero-proof) credentials, privacy policies negotiation, development of usable interfaces and privacy metaphors, etc. [7]. In addition, the identity management domain has begun to consider user-centric architectural and usability aspects, and to support user control to different extents, which is called user-centric identity management. For example, URL-based systems such as OpenID[1] allow users to choose the entity storing their personal data, OAuth enables users to decide on what pieces of information to share, Kantara User Managed Access[2] (UMA) lets an individual control the authorization of data sharing and service access made between online services on the individual's behalf, and card-based systems further allow users to include the pieces of information to be shared with a third party.

At the start of the PRIPARE project, it was realized that stakeholders use PbD and Security by Design with different definitions. PRIPARE provides its own definition of a privacy and security by-design process: An approach to System Engineering which takes into account privacy as well as measures to protect ICT related assets throughout the whole engineering process.

PbD is hailed as the solution to the digital world's privacy problems. It is usually presented as a set of principles that can be applied from the onset of systems development to mitigate privacy concerns and ensure compliance with Data Protection legislation. However, these principles often remain vague and rely on ambiguous concepts, and are hence difficult to apply to engineering systems [25]. There are many open questions and challenges that need to be addressed at both the management and development levels in order to define effective methods to integrate privacy into systems [24]. A variety of approaches are being used to address these privacy concerns throughout the lifecycle of products or systems.

- PIA and risk management processes: these will be discussed in more detail within the PRIPARE PSbD Methodology section.
- OASIS standardization efforts. OASIS is as a non-profit consortium that drives the development, convergence, and adoption of open standards for the global information society. There are currently two Technical Committees (TC) related to PbD:
  - The PMRM [17] TC (Privacy Management Reference Model and Methodology). The objective of PMRM (pronounced pim-rim) is to provide a methodology for developing operational solutions to privacy issues. A first specification of PMRM was issued in July 2013.
  - The PbD Documentation for Software Engineers TC (PbD-SE TC) [29]. The TC objective is to provide privacy governance and documentation standards for software engineers.

[1] http://openid.net/

[2] https://kantarainitiative.org/confluence/display/uma/Home

3 Converging to a Common Terminology

To enable the development of a methodology addressed to multiple stakeholders from different countries and industries, it is necessary to define a common terminology that facilitates communication to be straightforward and without ambiguities. There are many sources of terminology for the domains of privacy, security, and risk management. The most relevant sources for terminology for PRIPARE are the ISO Standards [15, 16], the EU Data Protection Directive (DPD) [14], EU GDPR [13] (approved by the EU parliament) and PMRM [17].

Beyond the discussion of specific terminology, an initial decision was made in terms of terminology style. In the EU DPD [14], terminology is focused on the term "data" or "personal data". It defines, in its principles and articles, responsibilities of data controllers, and data processors. It also defines sensitive categories of data. The European Data Protection Supervisor (EDPS), as expected, also follows that naming convention that is also endorsed by the Article 29 Data Protection Working Party [19]. On the other hand, ISO talks about Personal Identifiable Information (PII). Looking at the definitions, both terms refer to the same concept but the wording is different. All concepts in the ISO standards are defined in terms of the PII: PII controller, PII processor, in the same way as the EU DPD does with "data". The OASIS PMRM [17] also makes use of the ISO wording.

Wording style had to be carefully chosen as only one style should be used within PRIPARE to avoid confusion. A survey among the participants of the consortium unanimously decided to adopt the EU wording style within PRIPARE.

A literature review conducted in the initial stages of the project revealed some terms that can be classified as elusive or controversial such as accountability, consent or informed consent, personal data, privacy or proportionality. Previous studies regarding these terms have been taken into account and discussed among project experts, after which a proposed definition was agreed upon by the project partners. The accepted definitions will be published and used within PRIPARE as a basis for further work.

4 PRIPARE's Principles

There are a variety of principles that are relevant for the PRIPARE project. The consortium has identified several sources such as the European DPD [14], the proposal for a new EU GDPR [13], OECD privacy principles [27] or Federal Trade Commission (FTC) FIPPs and had successful discussions regarding the most appropriate principles for the PRIPARE project. The focus on principles discussion was further refined towards discussing ideas and principles of data minimization, personal data, user-centricity, accountability, privacy and consent.

The security principles under discussion by the PRIPARE consortium included applying defense in depth, using a positive security model, avoiding security by obscurity, keeping security simple, and establishing secure defaults. The source for these principles is the Open Web Application Security Project (OWASP) [28]. The project consortium has accepted these principles preliminarily. The security principles may be further debated with stakeholders as the project progresses.

The principles of data protection included in the PRIPARE project for discussion came from the European DPD 95/46/EC [14] and from the Proposal for a new European GDPR [13] (discarding OECD and FTC's articulations). These principles include safeguarding personal data, proportionality and data minimization, compliance with the data subject's right to access and amend their personal data accountability, and the right to deletion. These principles are important in terms of the data lifecycle, from the collection of personal data (and an individual consenting to this collection of their personal data), to processing (and the right of the individual to object to this processing and the principle of proportionality), to the deletion of personal data (and the right of the individual to have his data retained only for a set time period and to have his data erased after this time). To date, the project consortium has agreed on the principles listed. However there may still be a need for the PRIPARE project to include a reference to the use of state-of-the-art technologies and the need for engineers to build in new technological solutions to minimize privacy risks. The data protection principles, including issues such as "what is meant by consent?" will be further discussed with stakeholders as the project progresses. The draft of the EU GDPR, among multiple other changes, modifies the notion of consent to define it as explicit and informed, rather than implicit. The PRIPARE project will take these new developments into account.

Besides security and privacy principles, the consortium has also discussed the notion of privacy itself within PRIPARE. Privacy is certainly not a universal concept that can be applied across all technologies and all situations. Finn et al. [20] argue that current attempts to capture the complexities of privacy issues in reactive frameworks are inadequate. They state that "Rights to privacy, such as those enshrined in the European Charter of Fundamental Human Rights, require a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions, infringements and problems." Finn et al. suggest that Clarke's taxonomy is no longer adequate for addressing the range of privacy issues that have arisen with regard to a new and emerging set of systems and technologies. They therefore suggest an approach that encompasses seven types of privacy: privacy of the person, privacy of behavior and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association. This approach is beneficial in terms of navigating the various definitions of privacy in the literature to date. Rather than focusing only on personal data and personal communications, as has been the case to date in data protection legislation, the taxonomy proposed ensures that different types of privacy are protected. This is important in relation to PIAs, which should take into account all seven types of privacy. With regard to the PRIPARE project, it would be beneficial to keep this taxonomy in mind when thinking about Privacy by Design. Rather than getting caught up in the myriad and diverse definitions of privacy, basing the PRIPARE methodology on this taxonomy of seven types of privacy will move the debate forward as opposed to reinventing the wheel.

Accountability, as one of the EU DPD principles, was largely discussed as it has become a widely debated topic in recent years (in relation to privacy and data protection). EU discussions on accountability suggest that current legal regulations for protecting privacy are inadequate and that without a change in the current direction, the problems of data protection are set to continue. Furthermore, commentators in the field have suggested that "Accountability can form the focus for dealing with issues of scale in regulation, privacy risk assessment, self-regulation through certification and seals and foster an environment for the development of new technologies for managing privacy" [26]. Finally, accountability is tied together with legal compliance and the idea that those who control data should, on request, be able to show compliance with data protection legislation. Although these discussions place accountability at center stage, the practicalities of achieving accountability in practice are left open to further debate. For the purpose of the PRIPARE project, the definition of accountability that will be used is the one that appears in the EDPS glossary: "The principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities" [18]. However, the consortium is aware that there is much more to accountability than that which is listed in the quote (as already outlined in this paragraph).

The starting point of PRIPARE's methodology is the idea of minimizing the trust that users need to place on the data controllers or data processor which will be collecting, storing and processing their personal data. This principle implicitly ensures that the data minimization principle is fulfilled, since the best approach to minimize trust is to minimize the amount of data that needs to be entrusted.[3] The methodology will seek to minimize the amount personal data distributed to potentially untrustworthy parties, which in turn minimizes the risk of privacy breaches.

5 PRIPARE PSbD Methodology

PRIPARE will adopt identified best practices on PIAs and risk management processes to provide an unobtrusive methodology that will complement existing system development and project management methodologies. This way PRIPARE's methodology or reference model will ensure and ease the process of building privacy-friendly systems, bridging the gap between the abstract notion of Privacy by Design and the concrete system designing and building process.

PRIPARE's PSbD methodology aims to be holistic. This means that it can be applied to systems or subsystems that compose it, even those being designed separately; it must be adaptable to the specific aspects of each domain specific standard; and it must also take into account the various types of systems, from the small to huge applications.

A recent PIA framework developed for RFID has been cited as being a "landmark PbD document" [8]. The framework is the first of its kind to be sector-specific and developed by industry. It provides guidelines on how to process data specifically

[3] "Protecting privacy by minimizing trust" is an on-going work from some of PRIPARE partners that will be published in the future.

related to RFID applications, and how to assess privacy and data protection issues through PIAs. In order to be effective, PIAs need to move beyond legal compliance checks in order to "offer a prospective identification of privacy risks before systems and programs are put in place," and that they "have to consider privacy risks in a wider framework which takes into account the broader set of community values and expectations about privacy" [9].

PIAs should not be considered as simply legal compliance checks, which ask: If we did X, would we be in compliance with the law and the fair information principles upon which the law is based? Nor should they be considered to be privacy audits used to assess existing technologies, although, as Wright argues, a PIA can enable an organization to demonstrate compliance with legislation in the case of a privacy audit or complaint. Undertaking a PIA can "provide evidence that the organization acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation" [10]. A 2007 Linden Consulting report [9] for the ICO states that they are most useful for new programs, services or technologies. However, they are not simply used to warn against potential risks but also to mitigate these risks, and to change the development process accordingly. PIAs, therefore, move beyond the legal compliance to assess and address the "moral and ethical issues posed by whatever is being proposed" [11]. The Ontario Data Protection guidance states that the "cyclical nature of the information life cycle must be supported by appropriate policies, practices, procedures, tools and contracts". With reference to this life cycle of information, the guidance states that "risk must be properly identified, minimized to the extent possible and appropriately managed where it can't be eliminated" and "a proper contemplation of the information life cycle includes these concepts". A privacy impact assessment is one of the ways that the information life cycle can be managed and privacy risks minimized [12].

Wright suggests that there is currently a "growing interest in Europe in privacy impact assessment" [10]. The UK introduced the first PIA methodology in 2007, although PIAs have been used in Australia, Canada, New Zealand and the United States since the mid-1990s. Conducting a PIA is now mandatory for government agencies in the UK, Canada and the US. It has been found that "unless they are mandatory, many organizations may not undertake them even though their projects, technologies or services have serious privacy impacts" [10]. In terms of best practice, Wright concludes that a PIA process should include:

- An assessment of privacy risks an organization might face in relation to a new project
- A process of engaging stakeholders (including external stakeholders);
- Examples of specific risks, recommendations and an action plan;
- Third party reviews and benchmarks that organizations could use to test how well they are following the process,
- Publication of the PIA report and PIA updates if there are changes in the project.

PRIPARE will embrace and incorporate this view of PIAs in its procedure and reference model approaches. Ideally, a PIA should include (or be complemented by) a privacy risk analysis. Inspiration can be drawn from the security area which has a long experience in risk analysis. Risk analyses in this area typically includes well identified steps such as the definition of assets, the identification of threats, vulnerabilities, attacks, etc., leading to a decision making phase (risk acceptance, mitigation, avoidance, etc.). In the case of privacy, the decision should involve the choice of specific architectures and technologies (Privacy Enhancing Technologies, PETs). However PIAs differ from traditional security analyses in several ways: privacy properties are not similar to security properties (even if related), privacy itself is more difficult to grasp than security, and the decision making phase should involve all stakeholders. So the transposition of security risk analysis to privacy analysis is not straightforward and warrants serious thought.

In terms of best practice, Wright also suggests that, in addition to a third party review, accountability mechanisms, such as mandatory reporting requirements, should be implemented. Finally, Wright argues that tying PIAs to budget submissions for new projects and programs can ensure that a greater number of PIAs are actually undertaken, as well as enhancing accountability.

6 Complementing Current Methodologies with PRIPARE

From the beginning of a system until its disposal there are several phases that are considered as the *System Lifecycle*. The management of the different phases of the lifecycle usually follows some methodology. Different methodology types can be used to manage this life cycle and often project management and system development methodologies are mixed to provide an ad hoc methodology that can be used through the entire system lifecycle. Usual stages that can be found in project development methodologies are: Initiating, Planning, Executing, Monitoring & Controlling and Closing.

PRIPARE will have to provide a way to integrate its methodology steps into existing and widely-adopted project management methodologies as it will involve a series of tasks that affect not only the engineering process itself but also resource allocation and organizational requirements. Special focus will be made on the most extended PM methodologies: PMBOK[4] and PRINCE2.[5]

By addressing the integration of the PSbD methodology with the most extended system development and project management methodologies, PRIPARE will embed its principles (from the EU DPD, the new EU Data Protection Regulation Draft, Cavoukian's PbD Foundational Principles, OWASP security principles, etc.) and best practices (in PIAs, risk assessment, Security by Design) into new to-be-developed ICT systems. As it is impossible to address integration with all existing system development methodologies, this integration will be focused on methodology families or similar methodologies. The integration of methodologies will be addressed by using the general description of a methodology family (e.g. waterfall, iterative, incremental, prototype), or by using a representative methodology of the family (scrum as representative of agile methodologies). Complementing some of the methodologies may be

[4] http://www.pmi.org/PMBOK-Guide-and-Standards.aspx

[5] http://www.prince-officialsite.com/

quite easy as they have similar stages that can be matched. However, others (i.e. scrum) pose great challenges, such as:

- How to implement PbD in a methodology that has no design stage?
- How to reflect privacy requirements in a methodology that only uses user stories?

These issues will have to be tackled during the methodology design in order to provide an effective and applicable privacy and security-by-design software and systems engineering methodology. PRIPARE's methodology will have to be as unobtrusive as possible to encourage adoption. This can be achieved by making some steps optional or by being less prescriptive in *how* things should be done (however, an idea or an example of "how" should always be provided to ease the adoption process).

7 Concluding Remarks and Future Work

PRIPARE will consider existing PETs, risk management methodologies, PIA frameworks and other approaches to engineer and operationalize PbD (i.e. OASIS PMRM [17]) with the objective of providing an easily applicable methodology suitable for different stakeholders (engineers, decision makers etc.). This will defuse some of the worst PbD critics regarding its chances of adoption [21] such as: "More aspirational than practical or operational" and "Difficult to be implemented into engineering practices". It will also ensure that systems developed with the methodology will follow PRIPARE's security (OWASP) and EU GDPR data protection principles and privacy best practices. PRIPARE will develop a truly positive-sum methodological approach for engineering privacy into ICT Systems software design and development lifecycles that will be:

- Short, easy-to-understand, and easy-to-use,
- Principles-based,
- Provisioned with risk assessment standards,
- Designed to cover the whole system lifecycle,
- Flexible so it can adapt depending on the nature of the project and the information collected,
- Useful for different stakeholders,
- Engaged with engineering practices.

To achieve this, PRIPARE's methodology will embrace current PIA practices, extending them with the best PIA practices as determined by different studies and projects (e.g. [22, 23]). It will include a complete and standard risk assessment process to minimize privacy and security risks. The methodology will be designed to provide tasks, inputs, outputs and best practices that will cover complete lifecycle of systems, from its inception to its disposal, by complementing existing system development methodologies. Later the proposed methodology will be consolidated with feedback from stakeholders during training, presentation, and dissemination events, seminars and workshops of the initially defined methodology. In order to ensure the success of PRIPARE's methodology, several other initiatives other than the methodology definition itself will be carried out in parallel:

- Liaison with other EU projects,
- Provision of information and reference material for the general public, ICT educators, policy makers, and governmental and non-governmental bodies acting for human rights protection.

References

1. United Nations General Assembly: The Universal Declaration of Human Rights, Paris (1948)
2. United Nations General Assembly: The right to privacy in the digital age. Resolution A/C.3/68/L.45/Rev.1
3. Cavoukian, A.: 7 Foundational Principles of Privacy by Design. Information & Privacy Commissioner, Ontario, Canada
4. European Data Protection Supervisor (EDPS): Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (2010)
5. Article 29 Data Protection Working Party: Opinion 01/2012 Opinion 01/2012 on the data protection reform proposals, March 2012
6. RFID Industry, Privacy and Data Protection Impact Assessment Framework for RFID Applications, January 2011
7. Camenisch, J., Leenes, R., Sommer, D.: Digital Privacy: PRIME-Privacy and Identity Management for Europe. Springer-Verlag New York Inc., New York (2011)
8. Privacy by Design: “PbD based RFID PIA”. http://www.privacybydesign.ca/index.php/pbd-based-rfid-pia/
9. Linden Consulting Inc.: Privacy Impact Assessments: International Study of their Application and Effects, Information Commissioner’s Office, UK (2007)
10. Wright, D.: The state of the art in privacy impact assessment. Comput. Law Secur. Rev. **28** (1), 54–61 (2011)
11. Flaherty, D.: Privacy Impact Assessments: An Essential Tool for Data Protection, Canada (2000)
12. Cavoukian, A.: Privacy risk management: building privacy protection into a risk management framework to ensure that privacy risks are managed by default. In: Information and Privacy Commissioner, Ontario, Canada, p. 12 (2010)
13. European Commission, INOFFICIAL CONSOLIDATED VERSION AFTER LIBE COMMITTEE VOTE PROVIDED BY THE RAPPORTEUR 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), Brussels, 22 October 2013
14. European Parliament and the Council, Directive 95/46/EC of 24.10.1995 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 November 1995
15. International Organization for Standardization (ISO): Information technology – Security techniques – Privacy framework, ISO/IEC 29100:2011, First edition, Geneva, 15 December 2011
16. International Organization for Standardization (ISO): Information technology – Security techniques – Evaluation criteria for IT security, ISO/IEC 15408-2, First edition, Geneva, 1 December 1999

17. Organization for the Advancement of Structured Information Standards (OASIS): Privacy Management Reference Model and Methodology (PMRM), Version 1.0. July 2013
18. European Data Protection Supervisor (EDPS): European Data Protection Supervisor Glossary. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary
19. Article 29 Working Party. http://ec.europa.eu/justice/data-protection/article-29/
20. Finn, R., Wright, D., Friedewald, M.: Seven types of privacy. In: Gutwirth, S., Poullet, Y., et al. (eds.) European Data Protection: Coming of Age. Springer, Dordrecht (2013)
21. Rubinstein, I., Good, N.: Privacy by design: a counterfactual analysis of google and facebook privacy incidents. Berkeley Technol. Law J. **28**(2), 1333–1414 (2011)
22. Wright, D.: Making privacy impact assessment more effective. Inf. Soc. Int. J. **29**(5), 307–315 (2013)
23. European Commission - Directorate General Justice: Recommendations for a privacy impact assessment framework for the European Union, Brussels – London, November 2012
24. Spiekermann, S.: The challenges of privacy by design. Commun. ACM **55**(7), 38–40 (2012)
25. Gürses, S.F., Troncoso, C., Diaz, C.: Engineering privacy by design. In: Computers, Privacy & Data Protection (2011)
26. Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., Postigo, H. (eds.): Managing Privacy through Accountability. Palgrave Macmillan, Basingstoke (2012)
27. OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
28. OWASP Application Security Principles. https://www.owasp.org/index.php/Category:Principle
29. Organization for the Advancement of Structured Information Standards (OASIS): Privacy by Design Documentation for Software Engineers