Sarah Spiekermann-Hoff and Marie Caroline Oetzel

A systematic methodology for privacy impact assessments: a design science approach

Privacy-by-design through systematic privacy impact assessment: a design science approach

Marie Oetzel & Sarah Spiekermann
Institute for Management Information Systems,
Vienna University of Economics & Business
Augasse 2-6, 1090 Vienna, Austria

Abstract

For companies that develop and operate IT applications that process the personal data of customers and employees, a major problem is protecting this data and preventing privacy breaches. Failure to adequately address this problem can result in considerable damage to the company's reputation and finances, as well as negative affects for customers or employees (data subjects). We address this problem by proposing a methodology that systematically considers privacy issues by using a step-by-step privacy impact assessment (so called 'PIA'). Existing PIA approaches lack easy applicability because they are either insufficiently structured or imprecise and lengthy. We argue that companies that employ the PIA proposed in this article can achieve 'privacy-by-design', which is widely heralded by data protection authorities. In fact, the German Federal Office for Information Security (BSI) ratified the approach we present in this article for the technical field of RFID and published it as a guideline in November 2011. The contribution of the artefacts we created is twofold: First, we provide a formal problem representation structure for the analysis of privacy requirements. Second, we reduce the complexity of the privacy regulation landscape for practitioners who need to make privacy management decisions for their IT applications.

Keywords: Privacy impact assessment, privacy-by-design, security risk assessment, design science.

Introduction

Privacy maintenance and control is a social value deeply embedded in our societies. A global survey found that 88% of people are worried about who has access to their data; over 80% expect governments to regulate privacy and impose penalties on companies that don't use data responsibly (Fujitsu, 2010). At the same time, we witness a greater number of privacy breaches, including massive leakage of personal data to unauthorised parties. At a fast pace, technical systems are evolving to allow for unprecedented levels of surveillance. These developments demand new approaches to privacy protection.

One of these approaches is to require companies to conduct privacy impact assessments (PIAs). Like security risk assessments (ISO, 2008; NIST, 2002), a PIA calls for companies to conduct a systematic risk assessment where the privacy implications of their operations and personal data handling practices are scrutinized. PIAs aim to identify technical and organizational privacy threats and choose controls that mitigate those threats. Typically, the assessments should be done early in the development of an IT application, so that – following the principle of 'privacy-by-design' (IPCO, 2011) – privacy issues can be detected during product development and privacy-enhancing techniques and measures can be proactively built into systems. Ideally, the results of PIAs are made (at least in part) public on companies' or governments' websites so that institutions can demonstrate their 'accountability'. And data protection authorities can use PIA reports to understand the data handling practices of companies, their privacy efforts and legal compliance. The Madrid Resolution, which was signed by fifty global data protection officers and authorities, therefore encourages the implementation of PIAs (SDPA, 2009). The European Commission has integrated the concept of PIAs into the new regulation proposal for legal data protection (EC, 2012). And the Article 29 European Data Protection Working Party recently endorsed a PIA Framework for RFID (INFSO, 2011). In the US, the Federal Trade Commission has required both Google and Facebook to regularly conduct PIAs for the next twenty years.

Despite the strong political movement to establish PIA practices, their adoption is still rare, especially in Europe. While governments in Canada, Australia and the US use PIAs in some sensitive areas such as biometrics, health or homeland security, the private sector has not embraced the concept (Bennett and Bayley, 2007). This inaction can be explained by the fact that, until now, most PIAs have not been mandatory (Wright, 2011). But even if PIAs become mandatory, no standards exist on how to conduct PIAs; in addition, current approaches lack a clear methodology and easy applicability. As we will show below, none of the approaches describe a step-by-step process that a company could easily implement and integrate into its risk management processes (Wright et al., 2011).

To address the lack of conceptual completeness and rigorous methodology for existing PIAs, we propose a set of new constructs and a novel process reference model for systematically conducting PIAs. We extend prior work in this research area by transferring experiences and concepts from security risk assessments to the privacy domain. The goal of this PIA methodology is to complement existing risk management techniques and provide data controllers with a formal technique for analysing system-specific privacy requirements. To achieve this goal, we adopt the research approach of design science (Hevner et al., 2004; Gregor, 2006). Based on an existing theoretical knowledge base, design science research typically involves the construction and evaluation of new IT artefacts, constructs, models, methods, or instantiations to address organisational IT problems. In this article, we develop constructs for representing and evaluating privacy requirements as well as a new methodology for systematically running a privacy impact assessment.

For this purpose, the article proceeds as follows: The next section reviews the applicable knowledge base for PIAs. We look into current concepts of privacy and data protection, timely privacy assessment procedures and related methodologies for security impact assessment. The third section describes a new PIA methodology we developed and tested. Herein we define constructs, including the representation of privacy requirements in the form of privacy targets, and propose qualitative evaluation techniques to prioritize them with the help of protection demand categories. The fourth section includes an evaluation of our proposed methodology and constructs. In particular, we apply our PIA process model to the field of RFID technology, where we tested the model and established it through the German Federal Office for Information Security (BSI) as a guideline for the development of privacy-friendly RFID applications. We then discuss the limitations of PIAs, limitations of our approach and needs for future work. We close with a summary of our work reflecting on the contributions of this work from a design science perspective.

Addressing privacy issues: A review of the current knowledge base

The PIA methodology we present is based on a critical review of existing constructs and procedures. We reflect on the elements that informed our PIA methodology: existing privacy compliance procedures, privacy principles, regulations and assessment procedures such as security impact assessments.

Existing privacy compliance procedures and privacy-by-design

Legal compliance checks are the most commonly used privacy assessment procedures in most countries today. These compliance checks are based on laws that address data protection issues; the checks are conducted by companies' internal data protection officers, national data protection authorities or private auditing businesses. Some privacy compliance institutions also issue a privacy seal to companies that informs consumers about the privacy efforts of that company (i.e. (TRUSTe, 2011), (BBBOnLine, 2011), (EuroPriSe, 2011)). Despite their value, current compliance procedures face some challenges: First, they mostly take place at the end of the development of a system or even later, when the system is already up and running. Thus, they review existing system designs (Shroff, 2007), which can only be fixed in a bolted-on and often costly fashion. Second, they are not done by the engineers designing the system, but by auditors, lawyers or data protection officials, who just run through a checklist to determine legal compliance. These procedures are unable to influence more ‘code-based’ and rigorous privacy controls. Third, current compliance checks lack a standard procedure, partially because national data protection laws and sign procedures vary. In addition, most companies do not incorporate privacy management into the quality controls that are ensured by standardised risk procedures.

With mounting public pressure for privacy protection, PIAs are now being considered as possible complements to or replacements for these current procedures (EC, 2009). PIAs emerged during the mid-1990s in Australia, Canada, Hong Kong, New Zealand and the US (Wright et al., 2011). The first European PIA was initiated by the UK in 2007 (ICO, 2009). Stewart (1996) describes a PIA as follows: "In large measure, PIAs are directed not simply towards issues of legal compliance but the policy choices involved in answering the questions ‘ought we to do this?” Bennett and Bayley (2007) identified four common PIA requirements: (1) “conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified”, (2) “assess the impacts in terms broader than those of legal compliance”, (3) “be process rather than output oriented”, and (4) ”be systematic”. Against this background, we define a PIA as **a risk assessment methodology used proactively in the design or upgrade phase of an IT-system to make that system privacy friendly *and* compliant with data protection legislation.**

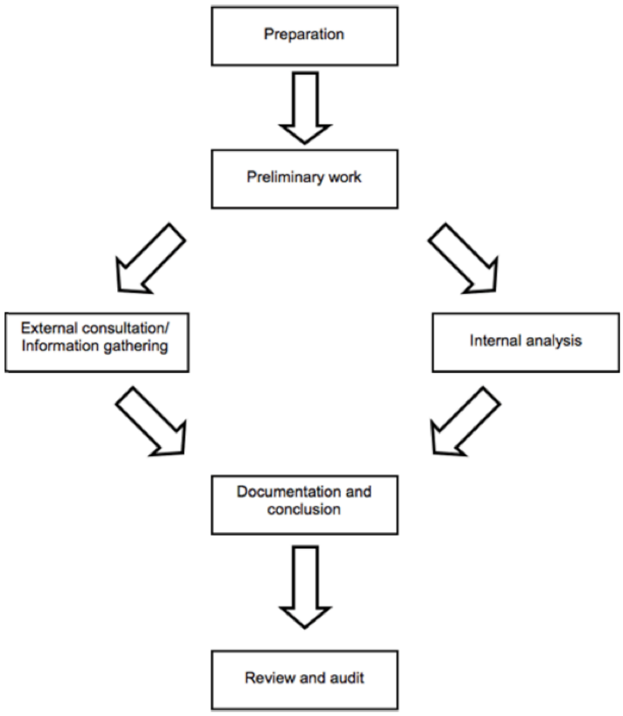
A PIA intends to overcome the shortcomings of legal compliance checks in several ways: First, a PIA is a process that accompanies all stages of a system development project, starting at the earliest possible moment and influencing system design decisions throughout the system development lifecycle (Bennett and Bayley, 2007; Clarke, 2009; Wright et al., 2011). Hence, it is not a one-time compliance check at the end of a project, but an ongoing requirements engineering exercise. Second, a PIA typically foresees the participation of technical and legal personnel as well as the integration of other relevant stakeholders, who can offer perspectives on an IT system beyond legal compliance (Jeselon and Fineberg, 2011). Third, because it offers a risk management approach that includes standardized procedures for how to assess and mitigate risks (e.g. (NIST, 2002; Seibild, 2006; ISO, 2008; BSI, 2008)), a PIA should lead to concrete technical improvements or design changes to a system. As a result, PIAs overcome the largely qualitative approach of the legal compliance domain.

PIAs are a crucial means to address one of the core concerns of today's privacy community, which is the establishment of privacy-by-design (Jeselon and Fineberg, 2011). *„Privacy by Design is an engineering and strategic management approach that commits to selectively and sustainably minimize information systems' privacy risks through pro-active technical and governance controls."* (Spiekermann, 2012). Privacy-by-design has been driven by the increasing recognition that a respect for user privacy cannot be realised through bolted-on measures that are only added to a system after it is deployed. Due to the rapid change in technology and the resulting inability to foresee all privacy issues, privacy measures must be integrated into the foundations of a system and PIAs are a key means to do so.

Risk assessment methodologies that tackle security and privacy issues

The core of a PIA is constituted by an impact assessment or risk assessment. Risk assessments typically follow a clear process of risk identification and mitigation. Consequently, such process orientation has also been identified as a key element of a PIA. Yet, existing PIAs largely fall short of it. As Figure 1a demonstrates, even the UK PIA handbook (ICO, 2009), which is considered a global "best practice publication" on how to conduct a PIA due to its valuable privacy question guide (Clarke, 2011; Wright et al., 2011), is methodologically not suited to be a process reference model. No input-output factors are described, and process steps are generic ("information gathering", "internal analysis"). As a result, people who conduct PIAs are uninformed about what to do when. No guidelines or conceptual tools support the risk assessment.

To our knowledge, the only PIA guideline with a valid process model is the PIA Framework for RFID, which was endorsed by the Article 29 Working Party and signed by the European Commission on April 6th 2011 (INFSO, 2011). This framework encourages European RFID application operators to run through a four-step PIA process: (1) describe their system landscape, (2) identify privacy risks, (3) mitigate those risks through appropriate controls, and (4) document the analysis and residual risks in a PIA report. This four-step methodology has been called a "landmark for privacy-by-design" by Ontario's data protection authorities, who invented the concept of privacy-by-design. Yet, in comparison to an equivalent security risk assessment (see Figure 1b), the PIA Framework for RFID is methodologically weak. We therefore reviewed existing security risk processes to inform the creation of a new PIA methodology.



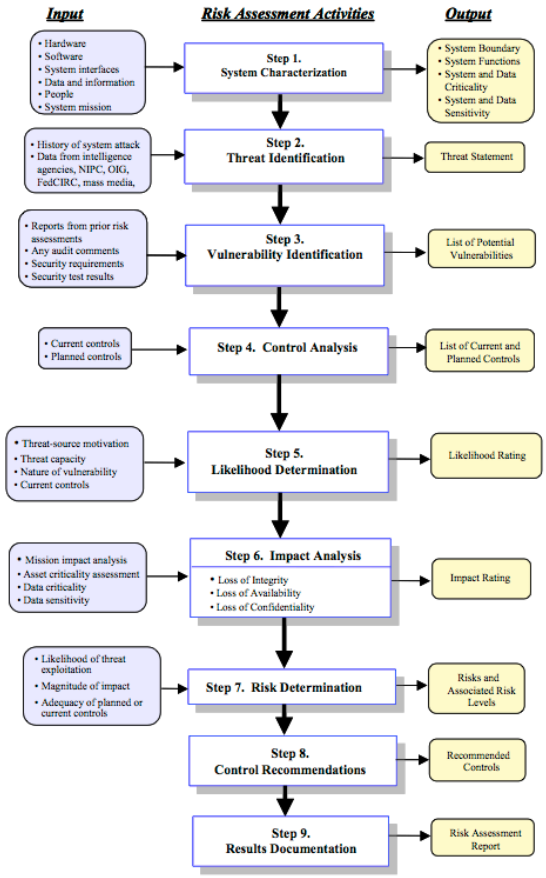


Figure 1a: State of the art in PIA methodology: UK PIA process (ICO, 2009)

Figure 1b: Benchmark for risk assessments: NIST security risk assessment process (NIST, 2002)

Standards and guidelines for information security management in organisations have been available for some time. The most prominent are the ISO/IEC 27000 series and NIST Special Publications 800 series. In Germany, the Federal Office for Information Security (BSI) provides industry with an IT Baseline Protection Catalogue ("BSI IT-Grundschutz") (BSI, 2011a). Similar to the NIST example depicted in figure 1b, these standards include interlocked steps that build on each other; to control for all relevant risks, the standards match each system threat with a respective control.

Most importantly, all of these standards offer guidelines that can be integrated into an organisation's risk management processes (see: (ISO, 2008), (NIST, 2002), (BSI, 2008)). The detailed steps and the artefacts of a security assessment enable a company to assess risk coherently. In addition, the standardised security risk procedures describe when each step should occur in the system development lifecycle. Security issues are considered early in the development and implementation of IT applications. The approach decreases bolted-on security functionality and promotes security-by-design.

Nevertheless, researchers describe the following problems that are inherent to existing security risk assessments and that we consequently need to keep in mind for our proposed methodology: focus on process and not on content and its quality (Siponen, 2006), focus on generic security requirements and thus disregard of company-specific requirements (Siponen and Willison, 2009), validation based on common practice and not on profound research methods (Siponen and Willison, 2009).

As privacy and security assessments are complementary, it is not surprising that both ISO/IEC 27002 and BSI IT-Grundschutz include privacy protection. Yet, analyzing these standards' privacy details, it turns out that the ISO standard leaves privacy policies and measures unspecified. The BSI IT-Grundschutz does apply security risk analysis to privacy principles. However, it reduces privacy protection to the concepts of anonymity, pseudonymity, unobservability and unlinkability (BSI, 2008). Thus, although the BSI approach (BSI, 2008) applies the security risk assessment method to privacy, it fails to embrace the wider spectrum of data protection principles inherent in the European Data Protection Directive or the OECD privacy guidelines.

Privacy principles and data protection regulation

To design a privacy analysis or PIA, one must first determine what needs to be protected (Rost, 2011). Unfortunately, *"Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests - from confidentiality of personal information to reproductive autonomy - and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name"* (Lillian Bevier cited in (Solove, 2005)). Daniel Solove (2002) conceptualized privacy along multiple dimensions: limited access to the self (building on Warren and Brandeis' (1890) concept of the 'right-to-be-let-alone'), secrecy (concealment of certain matters from others), control over personal information (in line with Westin's (1967) emphasis on information privacy), protection of one's personhood (in terms of protection of one's personality, individuality and dignity in the face of surveillance) and interpersonal intimacy. The UK PIA Handbook (ICO, 2009) is more abstract, stating that a PIA should consider not only the privacy of personal information, but also privacy of the person, personal behaviour and personal communications.

Because privacy is such a multidimensional construct, many privacy scholars argue that privacy extends beyond the notion of data protection, which the current legal environment focuses on (i.e. (Raab and Wright, 2012)). Scholars note that the OECD privacy guidelines (OECD, 1980) and European regulations often group data protection policies with the term 'privacy' but fall short of embracing privacy as a broader concept. For example, scholars criticize Article 33 of the proposal for a new EU data protection regulation. The article refers only to "*data protection* impact assessments"

(EC, 2012), but should mandate *privacy* impact assessments; as a result, the article may not apply to some areas where privacy is at stake.

We aim to resolve this battle of terms by asking whether the data protection rules outlined in the European data protection directive (and its successor regulation), OECD guidelines and Fair Information Practice Principles (FTC, 1998) sufficiently address the full spectrum of privacy threats that can be caused by IT systems. If data protection rules can sufficiently address or mitigate all *privacy* threats known to be caused by IT systems, we can say that - in the context of IT - data protection rules and privacy rules are effectively the same.

To date, (Solove 2006) has probably produced the most complete list of privacy threats. This list includes privacy threats observed over a century of US legal history. The threats include: cases of surveillance and false interrogation, cases of abundant and unlawful information processing in the form of data aggregation, personal identification, insecurity of data, unwanted secondary data uses or individual exclusion, cases where information dissemination lead to breach of confidentiality, unwanted disclosures, personal exposure, increased accessibility for private and governmental institutions, blackmail or appropriations and distortions, and cases of invasion in the form of physical or virtual intrusion and decision interference. We believe that most privacy scholars would accept this list of issues as a relatively complete picture of the privacy construct.

To further explore the similarities and differences between data protection rules and privacy rules, we combined Solove's list of privacy threats with data protection regulation. We then investigated whether rigorously following the current data protection regulation would sufficiently address all known privacy threats. If the data protection regulation is sufficient, then an electronic privacy effort could succeed by following data protection legislation. Appendix A summarises all elements of the current and proposed EU data protection regulation (EC, 1995; EC, 2012) and hence all data protection principles included in the OECD privacy guidelines (OECD, 1980) and Fair Information Practice Principles (FTC, 1998). The table leads to two conclusions: First, if companies take data protection regulation seriously, particularly by introducing high data quality and security standards, then *all* privacy threats identified by Solove (2006) are addressed. Second, data protection regulation provides people with additional information self-determination rights that go beyond the privacy domain. For our purposes, the first conclusion is the most important one. The table shows that data protection rules support the mitigation of all potential privacy threats. For example, Solove describes how privacy is harmed by data aggregation, which is the creation of a highly revealing and relatively complete profile of an individual from multiple data sources. If data protection rules are followed in the sense that data controllers avoid collecting data (P1.5), adhere to data minimization (P1.6), and restrict processing to pre-agreed legitimate purposes (P2.1 and P2.2), then it will be difficult for data controllers to lawfully create the kind of data aggregates that harm peoples' privacy.

Since table 1 demonstrates how all privacy harms can be addressed through existing data protection regulations, we argue that the PIA methodology we present is indeed a *privacy* impact assessment and not just a *data protection* assessment driven by a need for compliance.

PIA methodology and constructs

Against the background of the described knowledge base (PIA goals, risk assessment benchmarks, privacy constructs), we have developed a 7-step PIA methodology (figure 2). A PIA is triggered when either a new system is planned or an existing one is upgraded. The PIA can refer to a stand-alone application or a programme that is embedded in a wider networked backend infrastructure.

Privacy risk assessments are not necessary in all situations. They are only advisable if a system will use or generate personal data or when it can help to enrich adjacent databases that contain personal profiles. For this reason, the first step (step 1) of a PIA requires a thorough consideration of the system under scrutiny and its adjacent infrastructure. In line with thought leaders in the privacy design domain (Rost and Pfitzmann, 2011), we suggest that a PIA should then include a reflection of privacy principles that could be undermined by the system at hand (step 2). Or, in engineers' speak: it should include an identification of *privacy targets* that need to be reached through system design. Yet, as in all system development projects, not all system design targets are equally important. Some privacy targets may be crucial because ignoring them could seriously harm a data subject. But other privacy targets may have less priority, as their neglect would barely affect data subjects or companies. For this reason, step 3 of our proposed PIA process calls for privacy development targets to be weighed and assigned to *protection demand categories* that reflect their importance. Then, threats to each of the established privacy targets are identified (step 4). As we have seen in the security risk context, the identification of threats is central to risk assessment because each threat needs to be mitigated by one or several controls. If an explicit and detailed listing of all privacy threats is missing, controls cannot be individually assigned to counter those threats. Setting controls to counter each privacy threat one-by-one is the most important aspect of privacy-by-design (step 5). This exercise must be well documented in a PIA report (step 7) because data controllers and processors can use it to prove that they have made an effort to protect all relevant aspects of a data subject's privacy. Data controllers can also use this exercise to identify the threats that remain uncontrolled; these threats constitute the residual risks (step 6). The following sub-sections explain in more detail each step of the PIA methodology we propose.

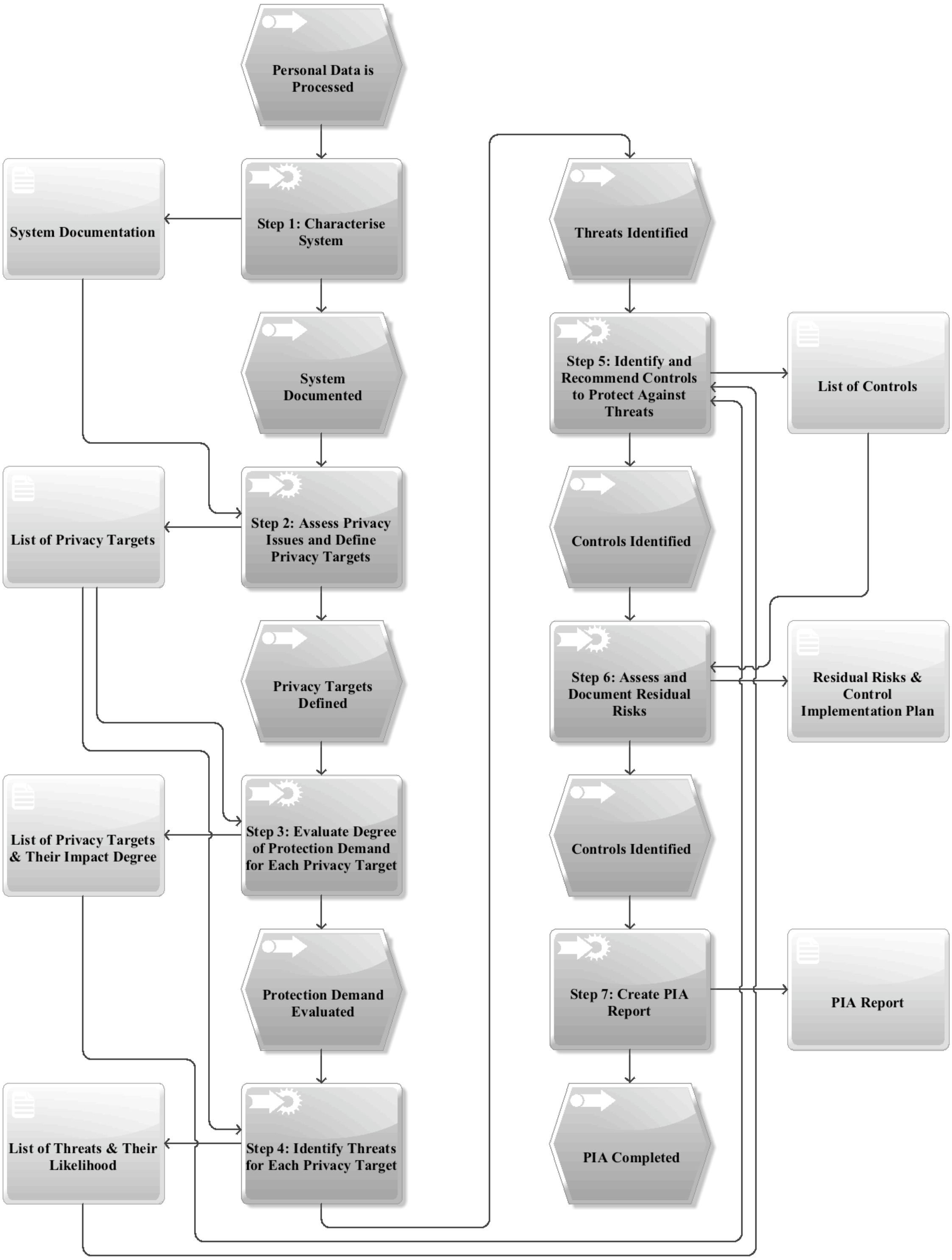


Figure 2. Event-Driven Process Chain for PIA Methodology

Step 1 – Characterisation of the system

The first step of a PIA aims to describe a system in such a comprehensive and detailed way that potential privacy problems can be detected. To minimize the risk that relevant information goes unnoticed, to facilitate privacy audits and to build on the system characterisation approaches of other risk assessment procedures (NIST, 2002; ISO, 2002; BSI, 2008; ISO, 2008), we recommend to document a system based on four views:

1. system view: application and system components, hardware, software, internal and external interfaces, network topology
2. functional view: generic business processes, detailed use cases, roles and users, technical controls
3. data view: categories of processed data, data flow diagrams (of internal and external data flows, including actors and data types)
4. physical environment view: physical security and operational controls such as backup and contingency

To be complete, the characterisation of a system should incorporate these four views and consider all system components and interfaces that are involved in the storage, processing and transfer of personal data. Each interface should be checked for whether it allows personal data to be transmitted to another component; the described data flows should contain all relevant actors that are involved in data transmission. Often, such documentation is already available if systems are well designed, are in a requirements-engineering phase or need to undergo security analysis. For a PIA, this documentation might need to be modified slightly to ensure that it emphasizes existing and potential data flows and data types more than system functionality. This emphasis on data flow models has also been outlined by the ISO PIAs in the financial industry (ISO, 2002).

The core challenge in this documentation phase of a PIA is to determine the right system boundaries and thus the assets (resources and information) that will need to be covered in the assessment. For example, if a retailer investigates an RFID-enabled inventory system for privacy implications, the retailer must determine whether to include loyalty program databases in the analysis. For the purpose of privacy analysis, we argue that a system boundary is reached when data flows end or none of the internally or externally adjacent systems are relevant for privacy. With the RFID inventory system application being easily linkable to a customer loyalty base, i.e. through barcodes, RFID data could be personally identified with reasonable effort. Hence a retailer would be well advised to include his loyalty programme in the privacy analysis of the inventory system.

Step 2 – Defining privacy targets

The purpose of a risk assessment is to understand what is at risk. Existing security risk assessments take the system characterisation from step 1 as a basis and then identify the assets described therein as security targets that need to be protected (e.g. ISO, 2008). They offer libraries of security targets that can be used by engineers and for assessment purposes. Unfortunately, such libraries only start to be elaborated for the privacy domain and are not yet standardised. Instead, legal catalogues (i.e. national privacy laws) and guidelines on privacy principles dominate the scene (i.e. FIPPs (FTC, 1998)). As we have seen above, these legal principles are not limited to data protection issues only but are able to embrace the full concept of privacy (see appendix A). In contrast to the above-mentioned libraries of security targets, legal privacy principles are difficult to use though for assessing concrete system functionality or describing the design of systems. This is because legal principles are semantically different and often more generic than concrete system functions that engineers can build or that can be scrutinized in a PIA. Just think, for example, of the legal principle of data quality required by Section 1 of the EU's Data Protection Directive (EC, 1995). Engineers think of data quality in much more concrete terms than what the law outlines; i.e. in terms of data integrity, precision, completeness, timeliness or consistency (Scannapieco et al, 2005). The translation (and back-translation!) of legal privacy principles into concrete, auditable and functionally enforceable privacy targets and subsequent system functions is hence an exercise that has been recognized as vital by privacy, security and legal scholars (Rost and Pfitzmann, 2009; Rost, 2011; ENDORSE, 2011).

For the purpose of our PIA methodology, we recommend referring to 'privacy targets' instead of 'privacy principles'. PIAs need to focus on concrete objects of analysis (i.e. system characteristics), and should help engineers identify specific design goals. The term 'privacy targets' supports this effort and is in line with the wording of security assessments that are a complement of and forerunner for PIAs. We acknowledge that both the EU Data Protection Directive (EC, 1995) and the ISO Standard for Privacy Architecture (ISO, 2011) refer to 'principles' where we use the term 'target'. But as table 1 shows, we also suggest formulating privacy targets as action items, similar to widely accepted modelling techniques like UML (Unified Modelling Language) and ARIS (Architecture of Integrated Information Systems). Formulating targets in this way promotes future action. By thinking in terms of actions that achieve development targets, we clearly depart from thinking in terms of principles when it comes to conducting a PIA.

That said, our privacy targets are directly derived from the established privacy principles formulated in the EU Data Protection Directive (EC 1995) and the EU's proposal for new data protection regulation (EC, 2012). This approach is in line with two official PIA standards we co-authored, namely the PIA Framework for RFID (INFSO, 2011) and the BSI PIA Guideline for RFID Applications (BSI, 2011b).

Privacy targets are derived from laws for several reasons: First, deriving privacy targets from laws implies that European companies running through all privacy targets will ensure that they comply with data protection regulations. Second, because European law is more exhaustive than many other guidelines (such as FIPPs (FTC, 1998)), deriving targets from laws produces a similarly exhaustive list of targets. And last but not least, laws reflect accepted standards of morality that society has chosen to accept. As a result, they constitute a more valid and reliable long-term foundation for system design than privacy targets that come out of an ad-hoc stakeholder process.

Many scholars point to the importance of stakeholder involvement in PIAs when it comes to the identification of privacy targets (Wright and De Hert, 2012). Rightfully, scholars critical of the law note that it lags behind technology developments or often does not cover all relevant ethical aspects of a specific technology (Van Gorp and de Poel, 2008). Stakeholders can therefore challenge whether targets derived from data protection laws adequately address the privacy issues inherent in a new technology. An example is a stakeholder process we conducted on RFID technology. We found that, in addition to the RFID privacy risks that are covered by the law, such as abundant data collection, consumers are also afraid of being constricted by the automation capabilities of the technology. In their private homes, people consider the ways that they deal with the objects they own to be private. The privacy target list for RFID-enabled consumer goods should therefore include a target such as, 'enabling the final control over automatic system reactions' (Spiekermann, 2008).

The target list in table 1 does not include technology-specific privacy targets. However, it is complemented by two privacy targets identified by (Rost and Bock, 2011): First, humans must generally be allowed to dispute machine conclusions (P5.5); second, in their communications with users, companies must uncouple the distinct ways that data is processed (P 1.3). Since these privacy targets are not embedded in most legal framework yet, we added them to the list.

In order to address the second of the above-mentioned problems of existing security risk assessments, at the outset of this second step, each privacy target needs to be described against the background of the respective industry or company context. The privacy target list in table 1 is a good baseline for assessing the privacy impacts of a system. But seen the wide spectrum of the privacy concept as well as national laws or industry-specific regulations more targets can and should be added. Where possible, a stakeholder process should challenge and discuss the applicability, meaning and exhaustiveness of the targets in a specific technology context.

Privacy Principles		Privacy Targets
P1 - Data Quality		
	P1.1	Ensuring fair and lawful processing through transparency
	P1.2	Ensuring processing only for legitimate purposes
	P1.3	Providing purpose specification
	P1.4	Ensuring limited processing for specified purpose
	P1.5	Ensuring data avoidance
	P1.6	Ensuring data minimization
	P1.7	Ensuring data quality, accuracy and integrity
	P1.8	Ensuring limited storage
P2 - Processing Legitimacy		
	P2.1	Ensuring legitimacy of personal data processing
	P2.2	Ensuring legitimacy of sensitive personal data processing
P3 - Information Right of Data Subject		
	P3.1	Providing adequate information in cases of direct collection of data from the data subject
	P3.2	Providing adequate information where data has not been obtained directly from the data subject (e.g. from third parties)
P4 - Access Right of Data Subject		
	P4.1	Facilitating the provision of information about processed data and purpose
	P4.2	Facilitating the rectification, erasure or blocking of data
	P4.3	Facilitating the portability of data
	P4.4	Facilitating the notification to third parties about rectification, erasure and blocking of data
P5 - Data Subject's Right to Object		
	P5.1	Facilitating the objection to the processing of personal data
	P5.2	Facilitating the objection to direct marketing activities
	P5.3	Facilitating the objection to disclosure of data to third parties
	P5.4	Facilitating the objection to decisions that are solely based on automated processing of data
	P5.5	Facilitating the data subject's right to dispute the correctness of machine conclusions
P6 - Security of Data		
	P6.1	Ensuring the confidentiality, integrity and availability of personal data storage, processing and transmission
	P6.2	Ensuring the detection of personal data breaches and their communication to data subjects
P7 - Accountability		
	P7.1	Ensuring the accountability of personal data storage, processing and transmission

Table 1. Privacy principles and privacy targets

Step 3 – Evaluation of protection demand for each privacy target

Not all of the privacy targets summarized in table 1 are applicable to all systems. For example, for some systems that collect data, such as sex sites or healthcare databases, people might be extremely sensitive about disclosure of their data to 3rd parties (P5.3). If limitation of disclosure was not ensured and such personal information leaked to the public, the reputation of both the person whose information was publicized and the company that leaked the data could be seriously damaged. In other situations, privacy targets may be legally required but not a priority for customers. For example, a telecommunications operator must facilitate the rectification and erasure of call data records (P1.8); if the operator failed to do so, the damage to the individual's finances and reputation would probably be less grave than in the example above.

Because the importance of privacy targets depends on context, companies running through PIAs should rank targets and identify priorities for their privacy architectures. To determine the right *level of protection demand,* companies can ask "What would happen if …?". As shown in table 2, we propose that companies use damage scenarios to answer this question. Both a system operator and its customers incur damage if privacy targets are not met. System operators might suffer financially or damage their company brand if privacy targets are not met. Data subjects can incur damage to their reputation, freedoms or finances.

The evaluation of privacy targets we propose differs from the more quantitative, asset-driven target evaluation of some security assessments (see e.g. (ISO, 2008)). Our approach differs because the consequences of privacy breaches are often of a 'softer' nature than security breaches; privacy breaches often relate to hurt feelings rather than something like the compromise of a computer system, which has a certain monetary value. For example, how do you quantitatively evaluate the consequences of a leaked body-scan? It is clearly difficult to quantify the personal consequence of privacy breaches. As a result, for each of five damage scenarios, we distinguish between limited, considerable and devastating consequences for an individual or a company. Depending on the highest level of consequence identified for a scenario, we then call for a corresponding degree of protection demand that can either be low, medium or high. In a later state of the assessment (step 5), this evaluation helps companies choose privacy controls that are aligned in strength and vigour. The approach we take here is similar to the security assessment procedures prescribed by the German Federal Office for Information Security (BSI, 2008). These procedures are proven to work well in practice because three consequence levels are cognitively more manageable and arguable than more complex scales.

Protection demand required for privacy target	**What could be impacted if privacy target was not met …?**				
	System operator perspective		Data subject perspective		
	Reputation or brand value	Financial situation	Social standing, reputation	Financial situation	Personal freedom
Low – 1	The impact of any loss or damage is **limited and calculable**.				
Medium – 2	The impact of any loss or damage is **considerable**.				
High – 3	The impact of any loss or damage is **devastating**.				

Table 2. Protection demand categories and perspectives

Step 4 – Identification of threats to each privacy target

At the heart of recognised risk assessment methodologies, one typically finds a listing of concrete threats to target assets and the probability that these threats will materialise. The assets under potential attack – in our case, the privacy targets – are analysed to determine why they are vulnerable. The causes of vulnerability and the threats are combined with the likelihood that the threats will occur. The result is a measure of the risk inherent in a system (for more detail on risk assessment methodologies, see (NIST, 2002; ISO, 2008)).

Our PIA methodology follows a similar approach. For each privacy target, we systematically *identify the threats* that could prevent us from reaching them. For example, privacy target P3.1 states that adequate information must be given to data subjects when data is directly collected from them. This target could be threatened in multiple ways: Companies may not give customers a privacy statement and thus fail completely to inform them. But companies may also fail to include the right information in a privacy statement, such as who the data controller is, why the data controller collects the data, whether data is shared, who the data is shared with, who to contact in cases of redress, and so on. In a PIA, threats are primarily failures to comply with privacy laws or sector standards, which are outlined in the privacy targets. In addition, failures might occur when stakeholders are ignorant of practices that have been identified as relevant in the privacy target list. Threats can materialise when technologies do not have adequate privacy functionality or when processes and governance practices fail to protect privacy.

For a threat analysis to be complete and justifiable, the threats in the analysis must match the identified privacy targets. Threats that do not correspond to a privacy target are not justified. If any privacy targets do not have corresponding threats, either the targets are not relevant or the threat analysis may be incomplete. To ensure a high level of methodological control in a PIA, privacy targets and privacy threats can be matched by using a numbering scheme (see figure 3 for illustration).

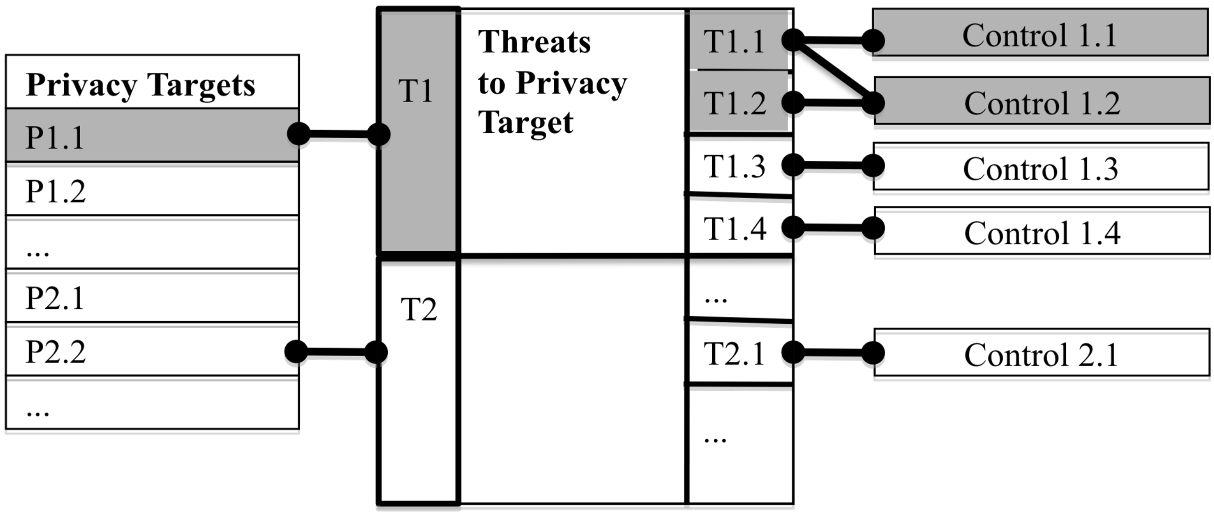


Figure 3. Controlled matching of privacy targets with threats and controls

Finally, not all potential threats are likely to occur. The probability that they become relevant depends on the technology, the IT-architecture, the people involved, the information governance of the company, the attractiveness and sensitivity of the personal data involved, the privacy education of employees and many other potential factors. Because so many variables can influence the incidence of a threat, security risk assessments determine threat probabilities. People who use security risk assessments determine what risks to tackle first based on these probabilities and the value of the underlying asset being threatened.

In the privacy domain we argue that such a gradual determination of threat probability as is done in security assessments is not advisable. This is, because if a human right such as privacy is threatened, it must be dealt with. The probability of a threat is therefore not important, but the question whether it is there or not. And if it is likely to be there, then a control must be determined to mitigate it. This is the next PIA step.

Step 5 – Identification and recommendation of controls to protect against threats

The crucial step in a PIA is to identify controls that can help to minimise, mitigate or eliminate each of the identified and likely threats. Controls can be technical or non-technical. Technical controls are directly incorporated into a system, whereas non-technical controls are management and administrative controls as well as accountability measures. Exemplary controls for each privacy target are summarised in Table 3.

Controls can be categorised as preventive or detective (NIST, 2002). Preventive controls inhibit violation attempts, while detective controls warn operators about violations or attempted violations. Because PIAs are intended to foster privacy-by-design, data controllers should focus on identifying and recommending preventive controls.

Privacy Targets		Controls Technical	 Administrative/Managerial
P1 - Data Quality			
P1.1	Ensuring fair and lawful processing through transparency		Providing accurate and up-to-date information, Making information accessible, Providing a privacy statement
P1.2	Ensuring processing only for legitimate purposes		Ensuring legitimacy of purpose
P1.3	Providing purpose specification		Providing an accurate and up-to-date purpose specification
P1.4	Ensuring limited processing for specified purpose	authentication, authorization, logging	Ensuring purpose related processing through policies and regular audits
P1.5	Ensuring data avoidance	minimal granularity	Ensuring data avoidance through policies and regular audits
P1.6	Ensuring data minimization	pseudonymisation, anonymisation, obfuscation, automated deletion routines	Ensuring data minimization through policies and regular audits, Providing and enforcing deletion rules
P1.7	Ensuring data quality, accuracy and integrity	data validation	
P1.8	Ensuring limited storage	automated deletion routines	Providing and enforcing deletion rules
P2 - Processing Legitimacy			
P2.1	Ensuring legitimacy of personal data processing		Ensuring obtainment of consent, Checking validity of consent
P2.2	Ensuring legitimacy of sensitive personal data processing		
P3 - Information Right of Data Subject			
P3.1	Providing adequate information in cases of direct collection of data from the data subject		Providing accurate and up-to-date information concerning (a) the identity of the data controller, (b) the purpose of processing, (c) the recipients of the data, (d) optional data
P3.2	Providing adequate information where data has not been obtained directly from the data subject (e.g. from third parties)		
P4 - Access Right of Data Subject			
P4.1	Facilitating the provision of information about processed data and purpose		Providing an interface that allows data subjects to send in a request for information, Ensuring timely processing of data subjects' request for information, Providing accurate and up-to-date information concerning (a) confirmation as to whether or not data relating to the data subject is being processed, (b) the purpose of the processing, (c) the categories of data concerned, (d) the recipients or categories of recipients to whom the data is disclosed, (e) the data undergoing processing and any information as to the data's source, (f) the logic involved in any automatic processing of data and automated decisions.
P4.2	Facilitating the rectification, erasure or blocking of data	authentication, authorization, logging	
P4.3	Facilitating the portability of data	export functionality	
P4.4	Facilitating the notification to third parties about rectification, erasure and blocking of data		Providing adequate and timely information about rectification, erasure and blocking of data to relevant third parties
P5 - Data Subject's Right to Object			
P5.1	Facilitating the objection to the processing of personal data		Providing an interface that allows data subjects to send in an objection, Ensuring timely processing of data subject's objection
P5.2	Facilitating the objection to direct marketing activities		
P5.3	Facilitating the objection to disclosure of data to third parties		
P5.4	Facilitating the objection to decisions that are solely based		
P5.5	Facilitating the data subject's right to dispute the correctness of machine conclusions		
P6 - Security of Data			
P6.1	Ensuring the confidentiality, integrity and availability of personal data storage, processing and transmission	technical information security controls	Administrative/managerial information security controls
P6.2	Ensuring the detection of personal data breaches and their communication to data subjects	technical information security controls	Providing adequate and timely information about personal data breach to data subject
P7 - Accountability			
P7.1	Ensuring the accountability of personal data storage, processing and transmission	authentication, authorization, logging	

Table 3. Privacy targets and exemplary controls

Controls that are more rigorous and extensive are also likely to be more costly and difficult to realize in practice. For this reason, we recommend three levels of rigor for controls: 1 - satisfactory, 2 - strong and 3 - very strong; for each privacy target, the level of rigor that is required depends on the degree of protection demand that was determined in step 3 of the PIA. For example, high (3) protection demands combined with likely threats should be mitigated with very strong (3) controls, while privacy targets with low (1) impact can be countered with a satisfactory (1) control. As figure 3 shows, one control can also address and mitigate multiple threats.

Step 6 – Assessment and documentation of residual risks

After the list of controls is written, the controls will need to be evaluated for feasibility and effectiveness. A cost-benefit analysis can be conducted, and stakeholders can be invited to discuss the acceptability of alternative controls. For example, suppose that a retailer wants to introduce RFID tags on products and has the control alternatives of killing tags at store exits or deactivating them with a password protection scheme. In this case, the retailer can discuss control options with customers to determine which approach is most acceptable for the market.

When potential controls are evaluated, data controllers can produce a control implementation plan that clearly identifies how each threat is mitigated and where threats remain unaddressed. Threats that remain unaddressed constitute the residual risk. A residual risk also exists if an implemented control reduces the impact of a threat but does not eliminate it completely.

Whether a residual risk is acceptable or a control option is postponed to a later stage of system deployment depends on the risk standards and norms of a design team or entire company (Naoe, 2008). In any case, the residual risks should be well documented in a PIA report (see next step); upper management, corporate risk management and IT-staff will be held accountable if privacy breaches occur.

Step 7 – Creating a PIA report

To date, no standards for good PIA reporting exist. The EU-PIAF project recently compared the main PIA reporting practices that exist (Wright et al, 2011). Extending their findings of what is typically included in PIA reports, we argue that the content of PIA reports should primarily meet target audiences' expectations. Manifold target audiences for PIA reports exist. Internally, a companies' corporate risk management, marketing staff, upper management and IT management must be aware of privacy risks. These groups must understand privacy risks not only because privacy breaches can lead to financial liabilities but also because privacy breaches can damage a companies' brand and force upper management to quit. At the same time, IT staff will probably be held responsible for any incidents that occur. Therefore, companies should have a strong interest in comprehensively documenting their privacy targets, threats, controls and residual risks; they should also ensure that their compliance with any relevant laws is regularly checked. IT staff will want to have the same information, but also must be able to quickly spot a system's weaknesses when a breach occurs. For them, quality documentation of the system and its data flows is essential (as outlined in step 1 above).

Externally, data protection authorities in many countries have the legal right to review PIA reports. Authorities may be put in a position where they must comprehend the system under scrutiny and judge whether system boundaries, privacy targets and threats have been properly identified and mitigated. Authorities also need to understand residual risks.

Finally, customers and the media might be interested in PIA reports. These groups want to understand the system and its purposes, customer control options and the core conclusions on threats and controls. For both, protection authorities and the media, some PIA quality signals could lead to acceptance that privacy work has been done. These signals include the reporting of stakeholder involvement and reporting on the start of a PIA process as part of system development. Finally, when things go wrong, everyone wants to know who is accountable and why a PIA failed to prevent a breach. Leading privacy experts have regularly called for accountability for privacy breaches (Alhadeff et al, 2011). Consequently, people will want to know when the PIA was conducted, how long the assessment took, who conducted it, and who is ultimately responsible for any breaches that occur.

Because PIA reports have such varied target audiences, who in turn have varied expectations, a PIA report should ideally contain the elements outlined in table 4. As shown in the table, it is advisable to produce two versions of a PIA report. The one for internal and auditing purposes provides much more content, some of which might be confidential; the version for the public can have less detail, but should be easy to understand. Furthermore, machine-readable PIA report standards should be developed so that both audits and consumer requests can be administratively facilitated. The P3P standard developed for privacy policies may be a good starting point for this exercise (Cranor et al, 2006).

	Data Protection Authorities	Company Staff	Customers	Media
General System Information				
System Overview	x	x		
System Boundaries	x	x		
System Purposes	x	x	x	x
Assessment Information				
Relevant Privacy Targets Identified	x	x	x	x
Relevant Privacy Threats Addressed	x	x		
Chosen Privacy Controls	x	x	x	x
Residual Risks Encountered	x	x	(x)	(x)
PIA Quality Signals				
Stakeholders involved	x	x		
Legal compliance checked	x	x	x	x
PIA start date/System's start date	x	x		
Accountability				
Person(s) involved in the PIA	x	x		
Organisation who conducted the PIA	x	x	x	x
Person who approved the PIA	x	x		
Privacy responsible in company	x	x	x	x
Date of PIA completion	x	x	x	x
Time frame of PIA validity	x	x		

Table 4. PIA reports and the target audiences' reporting expectations

Utility evaluation of the proposed artefacts

An important aspect of design science research is the evaluation of the proposed artefacts. To demonstrate the utility of our artefacts, we follow Hevner et al. (2004). We use the observational approach, in the form of workshops with IT industry experts, and the descriptive approach, employing the informed argument method and the scenario method. With the completion of these evaluation methods, we also address the above-mentioned problems of existing security risk assessments. We use profound research methods to evaluate content and quality of our proposed artefacts and not only rely on common practice.

Workshops with industry experts

Conducting interviews, in our case in the form of workshops, is one of the most important tools in qualitative research for gathering information (Myers and Newman, 2007). We worked with 6 industry experts holding different organizational roles relevant for PIAs: a general risk manager, an IT department manager, a technology innovations manager with a strong background in technical security management and several members of a governmental institution focused on information security, each of whom have a strong background in theoretical risk management.

In each workshop, we (1) explained our PIA methodology and constructs, (2) ran through the methodology with both the specific organisational context of the experts' internal operations and a fictitious scenario (BSI, 2011b, and (3) asked experts to suggest potential improvements to our proposed artefacts. We ensured that all three parts of the workshop were completed. Most of the workshops took 6 to 8 hours. The information was captured in the form of result protocols.

All interviewees confirmed that the comprehensive documentation of a system, as required in **step 1,** would be necessary to complete a reliable PIA. But participants were concerned about the amount of time and labour that would be necessary to create a detailed system characterisation. Participants noted that such comprehensive documentation is not readily available in a typical company, where the main interest lies in producing a running application rather than a well-documented one. It was especially difficult for participants to agree about where the documentation of the system should end and thus to grasp the scope of the system characterisation. The best solution to this dilemma that the participants suggested was to focus on the flow of personal data. In this approach, the documentation would describe the system components and interfaces that are part of the flow but stop documenting components at the point where personal data comes to a rest.

In **step 2**, all of the participants highly valued the privacy targets (see Table 1). The privacy targets systematically structure the confusing and extensive landscape of privacy requirements in a way that IS practitioners feel confident working with. Most importantly, since most of them are initially covering the law, legal compliance is ensured through a PIA. This is important for industry since PIAs are costly and should at least ensure legal compliance. When participants discussed each of the privacy targets in detail (in the context of their personal operations as well as the fictitious scenario), their confidence increased and they viewed the targets as less complex. Nevertheless, the 'correct' interpretation of some of the targets remained a problem. In particular, target P1.1 'Ensuring fair and lawful processing through transparency' resulted in discussions on how to interpret 'transparency' and how transparency can be ensured. Interestingly, this problem of 'correct' interpretation was not considered to be insurmountable; discussions always led to a certain interpretation. All participants admitted that they were not aware of most of the legal requirements coming into the discussion. The participants recognised that they would need to invest in training and additional personnel to foster the understanding of privacy issues throughout their organisations.

In **step 3**, where the assessment requires data controllers to evaluate how much protection each privacy target requires, participants agreed that a qualitative approach is the most feasible. As noted above, evaluating the impact of a privacy breach is different from evaluating the impact of security breaches; for example, a security breach such as a loss of availability might be easily quantified in terms of business losses. The two perspectives (operator and data subject; see Table 2) we proposed were considered to be very helpful for evaluating the 'soft' factors that are typically affected by privacy breaches. Nevertheless, participants with technical background, who were used to evaluating system failures quantitatively, had more difficulty working through this step than stakeholders with a risk management background. The latter stakeholders mainly considered the operator perspective, focusing on threats like damage to a company's image; technical stakeholders, meanwhile, focused on technical issues and omitted administrative issues. For both sets of stakeholders, significant effort was required to take on the data subject perspective and properly evaluate the relevant criteria; this finding emphasises how important it is that stakeholders explicitly adopt a second perspective. After discussing some of the privacy targets, stakeholders grew accustomed to the alternative way of thinking and reasoning about privacy issues, and they assigned the three levels of protection more easily.

For the evaluation of the likelihood of threats in **step 4**, the workshops led us to again adopt a qualitative approach. Although participants considered assigning a quantitative probability to each threat, the nature of most of the threats did not make this approach feasible. Thus, we settled on a simple differentiation in which each threat was labelled "likely" or "unlikely".

Most participants viewed the identification of controls in **step 5** as straightforward. Although they were not familiar with the concept of privacy-by-design, they agreed that privacy controls should be identified as soon as possible in the system development process. Participants lacked knowledge about the privacy-enhancing control options and measures that can help to realise a privacy-by-design approach. For example, participants did not know that they could implement pseudonymisation or anonymisation measures to fulfil the data minimisation requirement (see Table 3). Moreover, our interviewees from companies' IS departments recognized that privacy experts had never been part of their project teams; these experts might have brought significant knowledge and perspective to the system development lifecycles.

Participants were confident that they could document residual risks and set up an implementation plan of the identified controls in **step 6**; these actions resemble existing risk management processes, and they do not involve any privacy-specific procedures. In contrast, some participants were strongly concerned about the publication of a PIA report as required in **step 7**. Although they were concerned about revealing detailed and confidential information to the public, they agreed that the results of a PIA should be published. In addition, they agreed that external parties like data protection authorities and customers should be informed about the reasoning that lead to these results. Based on the workshops, we concluded that two versions of a PIA report should be written: a detailed report for internal use and audits from data protection authorities and a report that clearly summarises the results for customers and the media (see Table 4).

Three scenarios and exemplary PIAs

One way to prove the utility of a new method is to "construct detailed scenarios around the artefact" (p. 86 in Hevner et al., 2004). We therefore applied our methodology to three scenarios that involve a new RFID application: (1) a retail scenario involving an RFID-enabled loyalty card and tagged products, (2) a public transport scenario using RFID-enabled tickets and pay-per-use models, and (3) an automotive scenario involving an RFID-controlled assembly and an RFID-enabled employee access card. A very detailed description of these three scenarios and the application of our methodology can be found in (BSI, 2011b).

The defined privacy targets and protection demand categories were taken as-is from the scenarios; however, we added a list of 60 threats and 27 controls that are feasible in the context of RFID applications. All three scenarios were discussed with the interview partners mentioned above as well as an additional industry expert from the automotive sector and the RFID industry association. We then conducted exemplary PIAs for all three scenarios by using our methodology and constructs. As a full description of the scenarios and their respective PIAs is not in the scope of this paper, we refer the reader to the BSI's PIA guideline (BSI, 2011b). In the following section, we briefly describe some key findings of the exemplary PIA for the retail scenario. These key findings have consequences for the design of RFID applications in the retail sector and for related business processes. Thus, they lead to adaptations for privacy-by-design in the areas of system design, function and process.

In short, the retail scenario is composed of an RFID-enabled loyalty card, tagged products, added-value services and RFID-enabled shop-floor applications such as smart trolleys, smart shelves, and self-checkout systems. After we considered privacy targets, we generated the following privacy-control recommendations: extensively inform customers about RFID technology, the customer data that is collected and how this data is processed so that customers know that they may be 'scanned' by RFID readers (P1.1); give customers the opportunity to choose whether they want to participate in RFID-based services; separate logistical data from customer data (P1.2 and P1.3); implement fine-grained access rights and regularly update assigned access rights (P1.2 and P7.1); implement deletion rules that delete or anonymise customer data that is no longer needed for the specified purpose (P1.5 and P1.3); offer personalised and pseudonymised loyalty cards to customers (P1.3); kill or deactivate all product tags during checkout, but do not kill a product tag if a customer explicitly requests the ability to use the product in conjunction with added-value services (P1.2 and P7.1).

Challenges for PIAs, our methodology and outlook

The utility evaluation of our artefacts already hints at some limitations of our methodology. First, we use a qualitative evaluation approach consisting of three levels (low, medium and high) to evaluate the protection demand level. As a result, we consider only the magnitude of risk, not the probability. We therefore recommend that external and internal stakeholders be involved in every step of the process; stakeholders can contextualise and define privacy targets, evaluate protection demand and identify and evaluate threats. This stakeholder involvement could be supported by introducing expert 'Delphi' technique judgements (Linstone and Turoff, 1975), which are often used in qualitative risk assessments. However, small and medium sized companies that lack the resources to accomplish comprehensive Delphi risk analyses could use our current approach.

Second, we do not offer any means or instruments to measure and analyse how well a step has been executed and if the resulting artefact is complete. Like security risk assessment standards, we leave judgement concerning the completeness and quality of the executed assessment to the assessors; we also recommend regular audits that can unearth remaining issues and initiate improvements to both the implemented assessment process and the application. However, software tools could help to ensure that the assessment steps and their resulting artefacts are complete. To provide useful tools to practitioners, we already implemented an instantiation of our artefacts in the form of a web application "intelligentPIA" (iPIA, 2011); we also plan to do case studies to further evaluate the utility of our proposed artefacts.

Third, in this research we focused on the development of a PIA methodology. We did not consider how our step-by-step methodology can be integrated into a company's existing risk management and system development process. Although we explicitly chose to base our methodology on existing security risk assessments to facilitate a seamless integration, we did not examine if and how such an integration can be realised. This examination would be an important subject for future work.

Conclusion

Following the design science research paradigm, the major contribution of this research is the development of a new set of artefacts. These artefacts help practitioners and researchers understand the relevant privacy regulation landscape and analyse and assess privacy issues by using a systematic step-by-step process. The PIA methodology helps practitioners realise the concept of privacy-by-design in their system development lifecycle. Specifically, the artefacts provide systematic support for representing privacy requirements in the form of privacy targets, evaluating the degree of protection demand of these targets and systematically identifying threats and adequate controls. The proposed privacy targets have been systematically derived from legal data protection requirements and privacy principles. Our PIA methodology is built on prior risk assessment experiences and research, especially in the security risk assessment area. The methodology can be verified because each step of the PIA process produces an artefact. Although the methodology is described on a level of detail that allows practitioners to reproduce it and transfer it to their operational environment, the methodology has been tested only in a theoretical context.

Because this methodology will be applied in varied contexts, we expect the artefacts to vary as well. We do not anticipate changes to the methodological design itself, but we do expect the methodology to be applied in different ways. In particular, the proposed list of privacy targets can and must be adapted to national or regional legislation and technology or industry-specific regulation.

We tested our proposed methodology and artefacts with the help of industry experts and three comprehensive scenarios. The participants of our workshops challenged our methodology's utility and helped us to improve it. To ensure that our methodology could be reproduced by practitioners, we worked with participants to flesh out our description of the methodology and its supporting artefacts. By conducting three exemplary PIAs for the scenarios and thus creating an expository instantiation, we were able to test the methodology's completeness and feasibility. The scenario approach also proved that data controllers can use our methodology to discover privacy issues and appropriate controls early in the design phase of system development, thereby achieving the goal of privacy-by-design.

Acknowledgements

We would like to thank the reviewers of an earlier ECIS conference article version as well as Dariusz Kloza for helpful comments on this work, the German Federal Institute of Information Security and the German Data Protection Authorities for their willingness to verify, discuss and publish our approach, Christian von Grone (CIO of Gerry Weber) and Pierre Blanc (IT Innovations Management at Carrefour) for helping us improve our constructs and apply them to the retail industry, Markus Sprafke for challenging our methodology for the automotive RFID industry, Wolf Rüdiger Hansen for integrating our methodology into PIA workshops for the RFID industry and finally Julian Cantella for editing the English version of this paper.

References

ALHADEFF J, VAN ALSENOY B, and DUMORTIER J (2011) The accountability principle in data protection regulation: origin, development and future directions. Proceedings of Privacy and Accountability. Berlin, Germany.

BBBOnLine (2011). BBBOnLine – BBB Accredited Business Seal. http://www.bbb.org/online/, accessed 5 December 2011.

BENNETT, C and BAYLEY, R (2007) Privacy Impact Assessments: International Study of their Application and Effects, Loughborough University, UK.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2008). Risk Analysis on the Basis of IT-Grundschutz, BSI Standard 100-3. https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html#doc471418bodyText3, accessed 20 March 2012.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2011a). IT-Grundschutz-Kataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html, accessed 29 February 2012.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2011b). Privacy Impact Assessment Guideline for RFID Applications. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf;jsessionid=4BE04C3871C6AEB0CD78E76F22F0153A.2_cid244?__blob=publicationFile, accessed 7 March 2012.

CLARKE R (2009) Privacy impact assessment: Its origins and development. Computer Law & Security Review 25, 123-135.

CLARKE R (2011) An Evaluation of Privacy Impact Assessment Guidance Documents. International Data Privacy Law 1 (2), 111-120.

Cranor, L. F., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., Schunter, M., Stanpley, D. A., Wenning, R. (2006). The Platform for Privacy Preferences 1.1 (P3P1.1) Specification - W3C Working Group Note 13 November 2006. http://www.w3.org/TR/P3P11/, accessed 1 March 2012.

Director of the Spanish Data Protection Agency (SDPA) (2009) Standards on the Protection of Personal Data and Privacy – The Madrid Resolution. 5 November 2009, Madrid.

ENDORSE (2011). ENDORSE Project. http://ict-endorse.eu/, accessed 1 March 2012.

EC (European Parliament and Council of the European Union) (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, L 281, 31-50.

EC (Commission of the European Communities) (2009) Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, Brussels.

EC (European Commission) (2010) A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final. 4 November 2010, Brussels.

EC (European Commission) (2012) 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. 25 January 2012, Brussels.

EuroPriSe (2011). EuroPriSe – European Privacy Seal. https://www.european-privacy-seal.eu/, accessed 5 December 2011.

FTC (Federal Trade Commission) (1998) Fair Information Practice Principles.

Fujitsu (2010). Personal data in the cloud: A global survey of consumer attitudes. http://www.fujitsu.com/global/news/publications/dataprivacy.html, accessed 20 March 2012.

GREENLEAF G (2011) Global data privacy in a networked world. Research Handbook of the Internet. Cheltenham, Edward Elgar.

GREGOR S (2006) The Nature of Theory in Information Systems. MIS Quarterly 30 (3), 611-642.

HEVNER AR, MARCH ST, PARK J, RAM S (2004) Design Science in Information Systems Research. MIS Quarterly 28 (1), 75-105.

Information & Privacy Commissioner of Ontario (IPCO) (2011). Privacy by Design. http://privacybydesign.ca, accessed 7 February 2011.

intelligentPIA (iPIA) (2011). intelligentPIA – A Privacy Impact Assessment Tool. http://www.wu.ac.at/ec/research/ipia, accessed 1 March 2012.

INFSO (European Commission, Information Society and Media Directorate-General) (2011) Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12 January 2011, Brussels.

ISO (International Organization for Standardization) (2002). ISO FDIS 22307 Financial Services – Privacy Impact Assessment.

ISO (International Organization for Standardization) (2008). ISO/IEC 27005 Information technology – Security techniques – Information security risk management.

ISO (International Organization for Standardization) (2011). ISO/IEC CD 29101.4 Information technology – Security techniques – Privacy architecture framework.

JESELON P and FINEBERG A (2011) A Foundational Framework for a PbD-PIA. Toronto, Ontario, Information and Privacy Commission Canada.

LINSTONE HA and TUROFF M (eds.) (1975) The Delphi Method: Techniques and Application. Addison Wesley, London.

MYERS MD and NEWMAN M (2007) The Qualitative Interview in IS Research: Examining the Craft. Information and Organization 17 (1), 2-26.

NAOE K (2008) Design Culture and Acceptable Risk. In Philosophy and Design - From Engineering to Architecture (VERMAAS PE, KROES P, LIGHT A and MOORE SA), pp 119-130, Springer Science + Business Media.

NIST (National Institute of Standards and Technology) (2002) Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30.

NISSENBAUM H (2004) Privacy as Contextual Integrity. Washington Law Review 79 (1), 119-157.

OECD (Organisation for Economic Cooperation and Development) (1980). Guidelines on the protection of privacy and transborder flows of personal data.

RAAB C and WRIGHT D (2012) Surveillance: Extending the Limits of Privacy Impact Assessments. In Privacy Impact Assessment (WRIGHT D and DE HERT P), pp 363-383, Springer Science + Business Media.

ROST M (2011) Datenschutz in 3D. Datenschutz und Datensicherheit - DuD 5, 351-354.

ROST M and BOCK K (2011) Privacy By Design und die Neuen Schutzziele. Datenschutz und Datensicherheit - DuD 35 (1), 30-35.

ROST M and PFITZMANN A (2009) Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit - DuD 33 (6), 353-358.

SCANNAPIECO M, MISSIER P, BATINI C (2005) Data Quality at a Glance. Datenbank-Spektrum 14/2005.

SEIBILD H (2006) IT-Risikomanagement. Oldenbourg Verlag, München, Wien.

SHROFF M (2007) Privacy Impact Assessment Handbook. Report, Office of the Privacy Commissioner, Auckland, New Zealand.

SIPONEN M (2006) Information Security Standards – Focus on the Existence of Process, Not Its Content. Communications of the ACM 49 (8), 97-100.

SIPONEN M and Willison R (2009) Information security management standards: Problems and solutions. Information & Management 46, 267-270.

SOLOVE DJ (2002) Conceptualizing Privacy. California Law Review 90 (4), 1087-1156.

SOLOVE DJ (2006) A Taxonomy of Privacy. University of Pennsylvania Law Review 154 (3), 477-560.

SPIEKERMANN S (2008) User Control in Ubiquitous Computing: Design Alternatives and User Acceptance. Aachen, Shaker Verlag.

SPIEKERMANN S (2012) [forthcoming] The Challenges of Privacy By Design. Communications of the ACM, Viewpoint.

STEWART B (1996) Privacy Impact Assessments. Privacy Law and Policy Reporter 3 (4), Article 39.

TRUSTe (2011). TRUSTe privacy seal. http://www.truste.com/, accessed 5 December 2011.

UK Information Commissioners Office (ICO) (2009) Privacy Impact Assessment Handbook (Version 2.0). London.

VAN GORP A and DE POEL IV (2008) Deciding on Ethical Issues in Engineering Design. In Philosophy and Design - From Engineering to Architecture (VERMAAS PE, KROES P, LIGHT A and MOORE SA), pp 77-89, Springer Science + Business Media.

WARREN SD and BRANDEIS LD (1890) The Right to Privacy. Harvard Law Review 4 (5), 193-220.

WESTIN AF (1967) Privacy and freedom. New York: Atheneum.

WRIGHT D (2011) Should Privacy Impact Assessments Be Mandatory? Communications of ACM 54 (8), 121-131.

WRIGHT D and DE HERT P (2012) Privacy Impact Assessment. Springer Science + Business Media.

WRIGHT D, WADHWA K, DE HERT P and KLOZA D (2011) A Privacy Impact Assessment Framework for data protection and privacy rights. Deliverable D1 of the EU PIAF Project - Prepared for the European Commission Directorate General Justice. Brussels.

Appendix A: Privacy targets and how they address activities that can create harm

	Privacy Targets	Sources	Solove 2006, A Taxonomy of Privacy: Activities that affect privacy (and can create harm)															
			Information collection		**Information processing**					**Information dissemination**							**Invasions**	
			Surveillance	Interrogation	Aggregation	Identification	Insecurity	Secondary use	Exclusion	Breach of confidentiality	Disclosure	Exposure	Increased accessibility	Blackmail	Appropriation	Distortion	Intrusion	Decisional interference
P1 - Data Quality																		
P1.1	Ensuring fair and lawful processing through transparency	(OECD, 1980; EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),	▒	▒					▒			▒			■		▒	▒
P1.2	Ensuring processing only for legitimate purposes	(EC, 1995; ISO, 2011; EC, 2012)	■	■								■					■	■
P1.3	Providing purpose specification	(OECD, 1980; EC, 1995; ISO, 2011; EC, 2012)					▒	▒			▒		▒					
P1.4	Ensuring limited processing for specified purpose	(OECD, 1980; EC, 1995; ISO, 2011; EC, 2012)					■	■			■		■					
P1.5	Ensuring data avoidance	(EC, 1995; ISO, 2011; EC, 2012)	■	■	■	▒	▒											
P1.6	Ensuring data minimization	(EC, 1995; ISO, 2011; EC, 2012)			■	■												
P1.7	Ensuring data quality, accuracy and integrity	(OECD, 1980; EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),														■		
P1.8	Ensuring limited storage	(EC, 1995; ISO, 2011; EC, 2012)				▒	▒											
P2 - Processing Legitimacy																		
P2.1	Ensuring legitimacy of personal data processing	(OECD, 1980; EC, 1995; FTC, 1998; ISO, 2011; EC, 2012)			▒													
P2.2	Ensuring legitimacy of sensitive personal data processing	(OECD, 1980; EC, 1995; FTC, 1998; ISO, 2011; EC, 2012)			▒							▒						
P3 - Information Right of Data Subject																		
P3.1	Providing adequate information in cases of direct collection of data from the data subject	(EC, 1995; FTC, 1998; EC, 2012)																
P3.2	Providing adequate information where data has not been obtained directly from the data subject (e.g. from third parties)	(EC, 1995; FTC, 1998; EC, 2012)																
P4 - Access Right of Data Subject																		
P4.1	Facilitating the provision of information about processed data and purpose	(OECD, 1980; EC, 1995; FTC, 1998; ISO, 2011; EC, 2012)							■									
P4.2	Facilitating the rectification, erasure or blocking of data	(OECD, 1980; EC, 1995; FTC, 1998; ISO, 2011; EC, 2012)							■							■		
P4.3	Facilitating the portability of data	(EC, 2012)																
P4.4	Facilitating the notification to third parties about rectification, erasure and blocking of data	(EC, 1995; ISO, 2011; EC, 2012)														■		
P5 - Data Subject's Right to Object																		
P5.1	Facilitating the objection to the processing of personal data	(EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),						■	■									
P5.2	Facilitating the objection to direct marketing activities	(EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),						■	▒								■	
P5.3	Facilitating the objection to disclosure of data to third parties	(EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),									■		■					
P5.4	Facilitating the objection to decisions that are solely based on automated processing of data	(EC, 1995; ISO, 2011; Rost and Bock, 2011; EC, 2012),																■
P5.5	Facilitating the data subject's right to dispute the correctness of machine conclusions	(Rost and Bock, 2011)														■		■
P6 - Security of Data																		
P6.1	Ensuring the confidentiality, integrity and availability of personal data storage, processing and transmission	(OECD, 1980; EC, 1995; FTC, 1998; ISO, 2011; Rost and Bock, 2011; EC, 2012)	■			▒	■			■	■		■	■	■	■		
P6.2	Ensuring the detection of personal data breaches and their communication to data subjects	(EC, 2012)					▒			▒	▒	▒						
P7 - Accountability																		
P7.1	Ensuring the accountability of personal data storage, processing and transmission	(OECD, 1980; ISO, 2011; Rost and Bock, 2011)					■			▒								

■ The privacy target **strongly** impedes the given activity and thus **strongly** reduces the harm that can be be created by the activity.

▒ The privacy target impedes the given activity and thus reduces the harm that can be created by this activity.