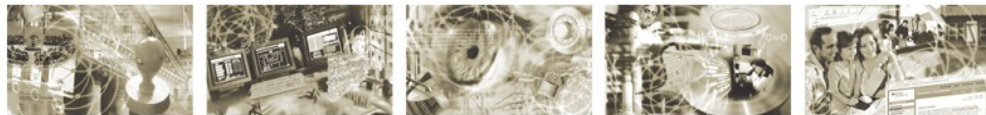




Bundesamt
für Sicherheit in der
Informationstechnik



Privacy Impact Assessment Guideline

Authors:

Marie Caroline Oetzel, WU Wien
Univ.-Prof. Dr. Sarah Spiekermann, WU Wien
Ingrid Grüning, BSI
Harald Kelter, BSI
Sabine Mull, BSI

Editor: Julian Cantella

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Tel.: +49 22899 9582-0

E-Mail: rfid@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2011

Contents

1	Introduction.....	5
2	Who needs to conduct a PIA and at what depth?.....	6
2.1	Who are considered RFID operators by the PIA Framework?.....	6
2.2	Initial analysis: Is there a need for privacy risk assessment?.....	7
2.3	Reporting of the Initial Analysis.....	9
3	Privacy risk assessment methodology.....	11
3.1	Step 1: Characterisation of the Application.....	12
3.2	Step 2: Definition of Privacy Targets.....	13
3.3	Step 3: Evaluation of Degree of Protection Demand for each Privacy Target.....	15
3.4	Step 4: Identification of Threats for each Privacy Target.....	18
3.5	Step 5: Identification and Recommendation of Controls Suited to Protect against Threats.....	25
3.6	Step 6: Assessment and Documentation of Residual Risks.....	35
4	Bibliography.....	36

List of Figures

Figure 1: Decision tree for initial analysis (Source: [EC2011]).....	7
Figure 2: PIA process reference model.....	11
Figure 3: Privacy risk assessment methodology.....	12
Figure 4: Systematically deriving privacy threats from privacy targets.....	18
Figure 5: Assessing and controlling privacy risks.....	25

List of Tables

Table 1: RFID application description (Source: [EC2011]).....	10
Table 2: Concrete privacy targets according to the EU Data Protection Directive 95/46/EC.....	15
Table 3: Protection demand categories.....	17
Table 4: Threats.....	23
Table 5: Threats to notification requirements.....	24
Table 6: Privacy-by-Design measures.....	27
Table 7: Controls.....	35

1 Introduction

In May 2009, the European Commission issued a recommendation that established a requirement to develop a framework for personal data and privacy impact assessments of RFID applications. This **Privacy Impact Assessment (PIA) Framework** was to be developed by industry in collaboration with civil society. Its goal is **“to help RFID Application Operators uncover the privacy risks associated with an RFID Application, assess their likelihood, and document the steps taken to address those risks”**.

By February 2011, the PIA Framework was developed by a consortium of major international industry bodies¹ and endorsed by the Article 29 Data Protection Working Party and the European Commission [EC2011]. RFID operators throughout Europe are now asked to comply with the co-regulatory data protection standard procedures outlined in the PIA Framework.

The goal of the present document is to explain the PIA Framework and to provide RFID application operators who need to conduct a PIA with an in-depth understanding of the framework's terminology and proposed procedures. For this purpose, the document is structured as follows: The next section (Section 2) explains who qualifies as an “RFID application operator” and what kind of responsibilities an operator has. Section 3 offers a step-by-step methodology for conducting a PIA. Privacy targets, threats and controls are described in detail; in addition, an evaluation process is outlined that qualitatively analyses privacy demands and threats so that adequate controls can be chosen. Three attachments to these guidelines exemplarily apply the methodology to specific scenarios from the retail environment, ticketing, manufacturing and access control.

The PIA methodology outlined in this document is a concretion of the highly generic process outline included in the PIA Framework. It is based on the technical guidelines for secure and privacy-friendly RFID applications that are provided by the German Federal Office for Information Security (BSI) [BSI2007]. By adhering to the PIA procedures outlined in this document, a company signals its commitment to optimise security and privacy operations according to timely standards in security management and EU data protection regulation. The goal is to ensure that companies gain a complete picture of their potential security and privacy threats as well as available security and privacy-by-design controls.

¹ The bodies who signed the PIA Framework include: Association of Automatic Identification and Mobility (AIM Global), The German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), The European Network and Information Security Agency (ENISA), GS1 Global, European Round Table (ERRT), European American Business Council and EuroCommerce. In addition, many organizations from Europe as well as from the US have participated in the formulation of the PIA Framework. These include: The German Federal Office for Information Security (BSI), Gerry Weber, Volkswagen, The Federal Office for Data Protection and Freedom of Information (BfDI), the European Digital Rights Association (EDRI), Vienna University of Economics and Business (WU Vienna), Carrefour (France), Oracle (US), Deutsche Post (Brussels) and McKenna Long & Aldridge (US).

2 Who needs to conduct a PIA and at what depth?

Before engaging in a PIA, companies operating RFID infrastructures must consider whether they are defined as “RFID operators” by the PIA Framework (who), the scope of their RFID applications (what) and the timing of the PIA (when).

2.1 Who are considered RFID operators by the PIA Framework?

The European Commission’s Recommendation indicates that *all* RFID operators should assess the impact of their operations on privacy and data protection. It defines an RFID application operator as a “natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application” [EC1995]. Yet RFID is a widely used technology that is already embedded in many of today’s products and service architectures. As a result, we must consider whether all RFID operators need to immediately analyse the privacy implications of their operations. What about tiny retailers or kiosks that may use RFID readers only to check out customers, replacing traditional barcode scanners with an RFID system? What about ski resorts that use RFID for access control? Are they all equally in need of a PIA?

The PIA Framework does not equally apply to all current RFID operators: The procedures have “**no retrospective effect**” and **apply only if “significant changes in the RFID application” are made**. Thus RFID operators need to run through a PIA only when they introduce a new system or make significant changes to their current operations. Significant changes are those that “expand” the application beyond its “original purposes” or lead to new “types of information processed; uses of the information that weaken the controls employed”.² For example, if a fitness club uses lockers with RFID keys and later personalises the keys so that premium members can use them for other purposes as well (i.e. paying for drinks), then the upgrade of the RFID functionality requires a PIA. The PIA is needed because the upgrade supplements the original locking function of the system with a payment function.

In the context of this fitness club example, another aspect of scope becomes apparent: whether the fitness club, who in this case is the RFID operator (the entity running the application), is responsible for conducting the PIA. After all, fitness clubs do not provide the technology; the function and technical architecture of the systems they use are often predetermined by system vendors. As the goal of a PIA is not only to identify privacy risks, but also to mitigate them technically, are customers who implement an “out-of-the-box” RFID system responsible for privacy controls because they “operate” it? Here, the definition of the RFID operator becomes important. **The RFID operator is the entity determining the purposes and means of operation.**³ In many cases, the RFID operator is the entity running the RFID application on its premises. However, because commercial entities are often not technically savvy and do not even specify the requirements for the standard software they operate, the system vendor or system implementer often carries the bulk of responsibility for conducting a PIA, becoming effectively the RFID operator. The

² The factors that would require a new or revised PIA include “significant changes in the RFID Application, such as material changes that expand beyond the original purposes (e.g., secondary purposes); types of information processed; uses of the information that weaken the controls employed; unexpected personal data breach with determinant impact and which wasn’t part of the residual risks of the application identified by the first PIA; defining of a period of regular review; responding to substantive or significant internal or external stakeholder feedback or inquiry; or significant changes in technology with privacy and data protection implications for the RFID Application at stake” ([EC2011], p. 5).

³ [EC2009], Art. 3(e).

responsibility of system vendors becomes particularly important when they offer turnkey RFID systems. In this case, system vendors need to conduct PIAs, because they are the ones who determine the purposes and means of those applications.

2.2 Initial analysis: Is there a need for privacy risk assessment?

Some companies *are* RFID operators in the sense of the PIA Framework but still don't need to conduct a PIA because they simply don't have a privacy problem. These RFID operators use RFID technology, but the data is never used for personal data processing or profiling and is also not linkable to personal data. If personal data is processed in conjunction with an RFID application, this data may differ in the *degree* of sensitivity. For example, some companies may process health information, payments or passport IDs with the help of RFID. Others just tag their cattle with RFID. Since privacy issues will probably vary for such different use cases, RFID operators should use an initial decision-tree analysis to assess whether and at what level of detail they need to conduct a PIA (see decision tree in Figure 1).

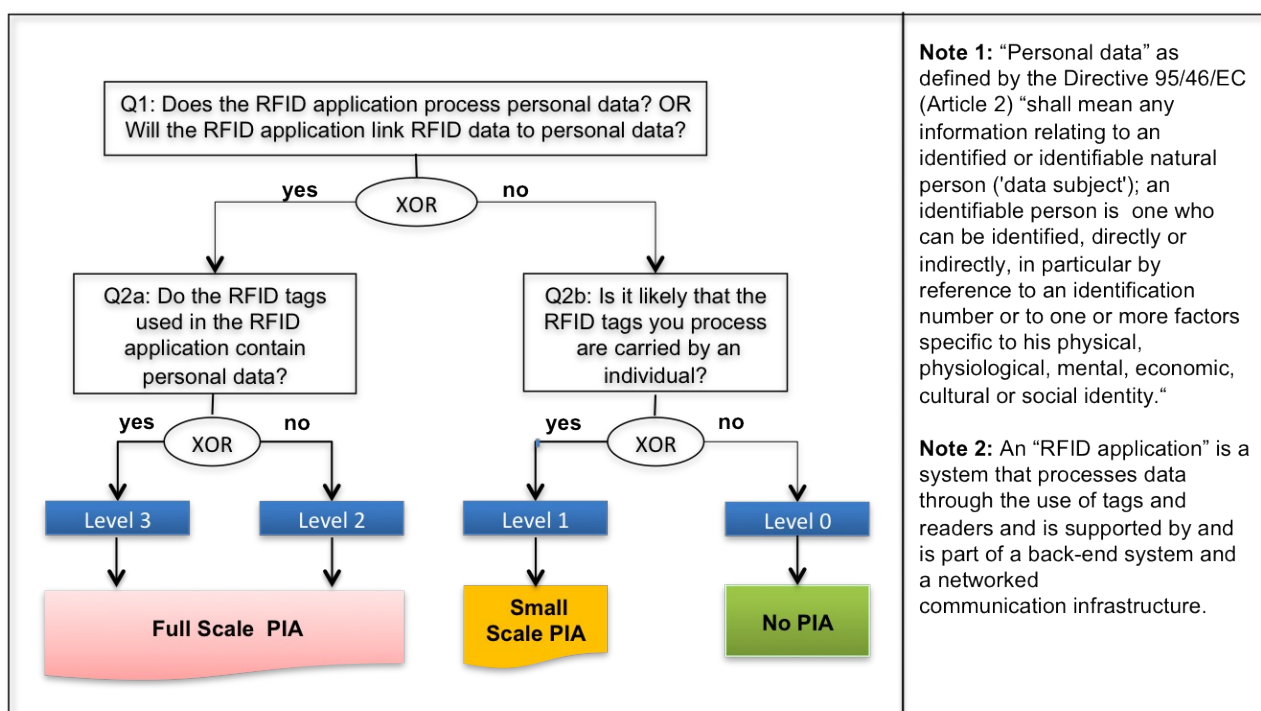


Figure 1: Decision tree for initial analysis (Source: [EC2011])

The key question for the initial analysis is whether the RFID application actually processes personal data or links RFID data to personal data. The issue of linking must be understood in the context of the PIA Framework's RFID *application definition*. An RFID application is "an application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure" ([EC2011], p. 23). Therefore, the **consideration of RFID back-end systems' links and sharing networks is important to determine whether a PIA is actually necessary and to what extent**. Considering networked back-end systems is important, because privacy problems often result only from the "secondary" processing of data; the secondary

processing of data typically occurs outside of the immediate application that initially collects and uses the data for a specific purpose. For example, a retailer may initially collect, store and process uniquely identified purchase item data for an RFID-enhanced inventory control application. These activities typically do not cause any privacy concerns. However, when the retailer decides that purchase data items should be combined with data from a back-end loyalty card system containing customer identities, a privacy problem is created and a PIA is warranted. Thus, **the RFID application borders for the PIA analysis include both the initial application collecting the RFID data plus all networked communication infrastructures that receive the RFID-based data for additional purposes.**

Finally, it is crucial to note that in the initial analysis phase, “personal data” is defined legally. A layman might think of personal data as information about an identified individual – a known person. In the legal sense, however, the definition of personal data is much broader. According to the EU Data Protection Directive, personal data is “any information relating to an identified *or identifiable* natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.⁴ An in-depth understanding of the concept of personal data is crucial in the RFID context. In its opinion WP 175 the Art. 29 group writes: “...when a unique identifier is associated to a person, it falls in the definition of personal data set forth in Directive 95/46/EC, regardless of the fact that the “social identity” (name, address, etc.) of the person remains unknown (i.e. he is “identifiable” but not necessarily “identified”).” [ART2010]. As a result, the Electronic Product Code (EPC) *could be* regarded as personal data and imply that all companies using the GS1 EPC standard **with the full serial number part** will automatically qualify as processors of personal data. The authors of this guideline document are aware that this interpretation of the EPC as personal data is still subject to debate. If a company does not handle personal data (right side of the decision tree), the next question (Q2b) in the decision tree aims to investigate whether a risk to privacy is still feasible. According to the stakeholder group that developed the decision tree for the PIA Framework and also according to the Art. 29 WP “potential privacy and security issues “... can still arise “if the tag is going to be carried by persons.” [ART2010]. Whether such issues are likely or not, must of course be determined in the context of a PIA. It is for this reason that the decision-tree includes the question of whether the RFID tags are likely to be carried by a person. If not, the RFID operator does not need to conduct a PIA (Level 0, no PIA). If yes, a small-scale PIA becomes necessary in order to check whether there is a likely threat to privacy and how this could be mitigated.

If a company does handle personal data (left side of the decision tree) in conjunction with its RFID application, it must answer a second question (Q2a) about personal data on the tags. If personal data is stored on the tags, the privacy analysis requires more detail. For example, both a health care system involving patient data and a retailer using unique purchase identifiers in conjunction with identifiable loyalty card data would have to answer “yes” to the question Q2a.

⁴“**Personal Data**” as defined by the Directive 95/46/EC (Article 2) ‘shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’. Additionally, WP 136 and WP 175 (section 2.2) of Art. 29 Data Protection Working Party should be considered, which detail the concept of personal data and qualify a unique number as personal data if it is carried by a person.

„**Sensitive personal data**“ is defined by the Directive 95/46/EC (Article 8) as any personal data that relates to (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Additionally, it is recommended to consider the context, too, when determining the sensitivity of personal data. Data that is not sensitive in itself may become sensitive in a specific context.

Two recurring questions on the decision tree are: why are there different levels of PIAs and how are these related to small- and full-scale PIAs. In fact, the terminology of “levels” was introduced to indicate the *level of detail* required for privacy analysis. Levels do not say anything about the amount of risk inherent in an RFID application.

Furthermore, the decision tree distinguishes between a full-scale PIA and a small-scale PIA. Again, full-scale vs. small-scale does not say anything about the risks that may be identified. The scale distinction was made so that companies (in particular, small and medium enterprises) that do not process personal data in relation to RFID data would not be overburdened by an extensive privacy analysis, even if they have to take some responsibility for passing on tags that are carried by individuals. “The phases in a small-scale PIA mirror those in a full-scale PIA, but a small-scale PIA is less formalized and does not warrant as great an investment of time and resources in analysis and information-gathering” [ICO2009]. The responsibility for conducting a small-scale PIA can probably remain with the person or team who introduces the RFID application and dispense with the stakeholder process that is recommended for a full-scale PIA. However, entities developing *PIA templates* for whole sectors or product- and service-lines should run through a full-scale PIA. Small-scale PIAs could potentially identify huge privacy risks within an RFID application. Full-scale PIAs could lead to the conclusion that the application has a privacy friendly system design and thus contains no likely threat to privacy.

2.3 Reporting of the Initial Analysis

Ultimately, the initial analysis must be reported. The PIA Framework states that the “initial analysis must be documented and made available to data protection authorities upon request” ([EC2011], p. 6). The documentation of the initial analysis should not only describe the RFID application at a superficial level, but also contain all information needed to judge the potential privacy impact of the system or conclude that there is no privacy impact. The requirement for this documentation implies that the description of the RFID application must contain detailed information about the method and purpose of data storage, processing and transfer. Table 1 shows what reporting elements must be contained in an RFID application description according to Annex I of the RFID PIA Framework.

2 Who needs to conduct a PIA and at what depth?

Report section	Description
RFID application operator	<ul style="list-style-type: none"> • Legal entity name and location • Person or office responsible for PIA timeliness • Point(s) of contact and inquiry method to reach operator
RFID application overview	<ul style="list-style-type: none"> • RFID application name • Purpose(s) of RFID application(s) • RFID application components and technology used (i.e. frequencies, ...) • Geographical scope of the RFID application
PIA report number	<ul style="list-style-type: none"> • Version number of PIA report (distinguishing new PIA or just minor changes) • Date of last change made to PIA report
RFID data processing	<ul style="list-style-type: none"> • List of types of data elements processed • Sensitive data processed?
RFID data storage	<ul style="list-style-type: none"> • List of types of data elements stored • Storage duration
Internal RFID data transfer (if applicable)	<ul style="list-style-type: none"> • Description or diagrams of data flows of internal operations involving RFID data • Purpose(s) of transferring personal data
External RFID data transfer (if applicable)	<ul style="list-style-type: none"> • Type of data recipient • Purpose(s) for transfer or access in general • Identified and/or identifiable (level of) personal data involved in transfer • Transfers outside the European Economic Area (EEA)

Table 1: RFID application description (Source: [EC2011])

3 Privacy risk assessment methodology

As with many modern quality management or business continuity activities, a risk assessment is validated by using a **process reference model**. A process reference model provides a procedure that ensures that privacy risks and mitigation strategies are identified. At a generic level, the PIA process reference model has been outlined in the PIA Framework and is depicted in Figure 2.

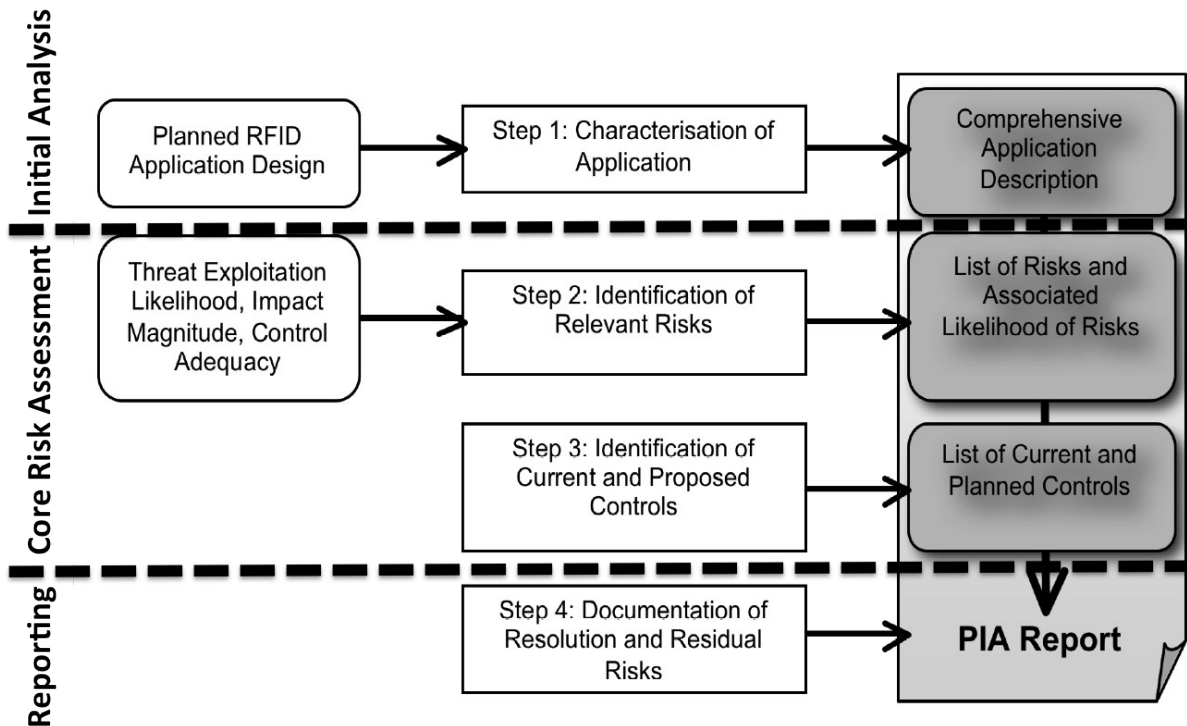


Figure 2: PIA process reference model

If the initial analysis concludes that a PIA is necessary and the RFID application description is completed (as described in Table 1), the first step of the risk analysis is completed. The next step (step 2, Figure 2) is to identify the privacy risks associated with the RFID application and to identify current or new controls (step 3, Figure 2) to mitigate those risks. The first two steps can be viewed as the “core” of a risk assessment; as such, companies should follow standard procedures for security and privacy risk assessments. Standard procedures include the German BSI's Technical Guidelines for Implementation and Utilization of RFID-based Systems [BSI2007] and their methodological specifications for different target application areas such as trade logistics [BSI2008], public transport [BSI2009] and employee cards [BSI2010].

In line with other security and privacy assessment standards⁵, the BSI privacy and security technical guidelines [BSI2007] assume that it is **vital to understand whether, how and how strongly RFID applications actually threaten privacy, and with what effect. After threats are identified, relevant controls are set to mitigate them.** For this purpose, RFID operators should complete the standardised and concrete risk assessment methodology described in Figure 3.

⁵ These include: [ISO2008], [ENISA2010] and [NIST2002].

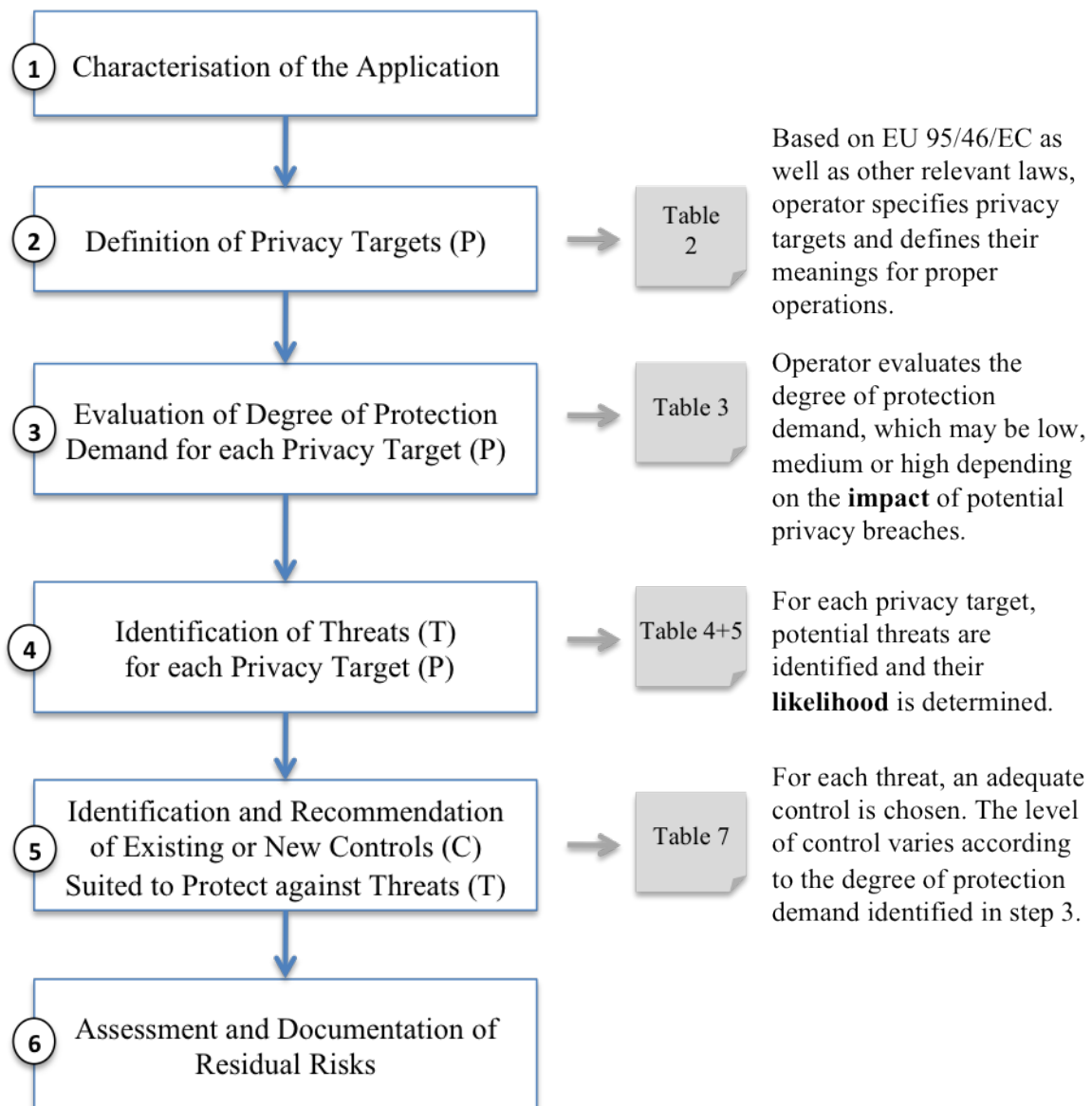


Figure 3: Privacy risk assessment methodology

When operators complete each of the steps outlined in Figure 3, they report their major conclusions. The conclusions, which may include details about the main privacy targets, the core threats and the core controls, should be documented in the PIA report.

3.1 Step 1: Characterisation of the Application

Operators can use the RFID application description (see Table 1) from the initial analysis as a starting point for the characterisation of the application.

From there, operators should complete an application characterisation that includes a detailed description of scenarios and use cases, systems and system components, interfaces, data flows and

involved parties. The characterisation should clearly identify the scope, boundaries and assets (resources and information) that need to be protected.

This information can be derived from requirements and design documents when the application is still in the initiation, design or development phase. If the application is already operational, relevant information can be collected from the production environment. Thus, information gathering is not restricted to a specific phase; information can be gathered throughout the privacy risk assessment process.

3.2 Step 2: Definition of Privacy Targets

The purpose of the risk analysis is to understand **what is at risk**. What is the privacy protection target? The PIA Framework specifies EU legislation as the starting point for risk analysis because any company's prime goal in evaluating privacy risks is to ensure legal compliance.

Framed legally, the European Data Protection Directive formulates nine privacy targets (P1 to P9), which are summarised in Table 2 (and included in Annex II of the RFID PIA Framework). These privacy targets correspond to sections I to IX of the EU Privacy Directive 95/46/EC from 1995. And their concretions (also included in Table 2) are taken directly from the EU Directive's legal articles.

If national law or industry-specific regulations go beyond the requirements of the European Data Protection Directive, additional privacy targets need to be added.

At the outset of the risk assessment analysis, every legal privacy target (P) needs to be defined against the background of the respective industry, company context or application domain. The legal text and its details should be applied to one's organisational context and to the RFID application at hand.

As shown in Table 2, all privacy targets (P) and concrete sub-targets are represented with a short key '*Pn.n*'. For example the privacy target "Safeguard of quality of personal data" is denoted as P1, and one of its sub-targets, the provision of purpose specification, is denoted as P1.2.

Threats (denoted as 'T') and controls (denoted as 'C') in Tables 4, 5 and 7 will later be linked with each of these privacy target keys (P1.1, P1.2, ... *Pn.n*). The keying schema is a common support mechanism for privacy and security assessments; the schema ensures that the risk assessment is methodologically rigorous and complete.⁶

⁶ [BSI2007], [ENISA2010].

3 Privacy risk assessment methodology

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name		Description of privacy target
P1	Safeguard of quality of personal data	P1.1	Ensuring fair and lawful processing through transparency ⁷	E.g. providing a description of the data processing activities required for product and service delivery, ensuring internal and external transparency. See Directive 95/46/EC, Section I, Article 6 (a).
		P1.2	Providing purpose specification and limitation	See Directive 95/46/EC, Section I, Article 6 (b).
		P1.3	Ensuring data avoidance and minimisation	e.g. processing only adequate and relevant personal information, non-excessive use of personal data. See Directive 95/46/EC, Section I, Article 6 (c).
		P1.4	Ensuring quality of data	E. g. ensuring accuracy, up-to-dateness, erasure or rectification of data that is incorrect or incomplete. See Directive 95/46/EC, Section I, Article 6 (d).
(P9)	Safeguard of quality of personal data AND Compliance with data retention requirements	P1.5	Ensuring limited duration of data storage	E.g. ensuring that data permitting identification of the data subject is not stored longer than necessary. See Directive 95/46/EC, Section I, Article 6 (e).
P2	Legitimacy of processing personal data	P2.1	Legitimacy of processing personal data	E.g. ensuring that consent, contract, etc. is available. See Directive 95/46/EC, Section II, Article 7 (a-f).
P3	Legitimacy of processing sensitive personal data	P3.1	Legitimacy of processing sensitive personal data	E.g. ensuring that explicit consent from the data subject, a special legal basis, etc. is available. See Directive 95/46/EC, Section III, Article 8.
P4	Compliance with the data subject's right to be informed ⁸	P4.1	Providing adequate information in cases of direct collection of data from the data subject	E.g. providing information about: identity of the controller, purpose of processing, recipients of the data, etc. See Directive 95/46/EC, Section IV, Article 10 (a-c).

7 Similar to [ULD2010], the Directive's Article 6, 1(a) "processed fairly and lawfully" is interpreted in terms of internal and external transparency.

8 In contrast to P1.1, which deals with information duties that are directed to a group of people (e.g. the public, the customers), P4 describes information duties vis-à-vis an individual data subject.

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name		Description of privacy target
		P4.2	Providing adequate information where the data has not been obtained directly from the data subject	E.g. providing information about: identity of the controller, purpose of processing, categories of data concerned, recipients of the data, etc. See Directive 95/46/EC, Section IV, Article 11.
P5	Compliance with the data subject's right to access, correct and erase data	P5.1	Facilitating the provision of information about processed data and purpose	See Directive 95/46/EC, Section V, Article 12 (a).
		P5.2	Facilitating the rectification, erasure or blocking of data	See Directive 95/46/EC, Section V, Article 12 (b).
		P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	See Directive 95/46/EC, Section V, Article 12 (c).
P6	Compliance with the data subject's right to object	P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	E.g. providing information before disclosure to third parties and/or use of personal data or direct marketing, so that objection is possible. See Directive 95/46/EC, Section VII, Article 14.
		P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	See Directive 95/46/EC, Section VII, Article 15.
P7	Safeguard of confidentiality and security of processing	P7.1	Safeguarding confidentiality and security of processing	<i>Here, security targets, which are defined in BSI's technical guidelines TG 03126, are relevant.</i> See Directive 95/46/EC, Section VIII, Articles 16 and 17.
P8	Compliance with notification requirements	P8.1	Compliance with notification requirements	See Directive 95/46/EC, Section IX, Articles 18 to 21.

Table 2: Concrete privacy targets according to the EU Data Protection Directive 95/46/EC

3.3 Step 3: Evaluation of Degree of Protection Demand for each Privacy Target

Even though all privacy targets are equally important for the regulator, they might have different degrees of urgency from a company perspective. For this reason, it is advisable to assess the level of privacy protection most feasible for an organisation.

In security assessments, security targets (i.e. the confidentiality of data) are often ranked according to the loss or damage that would result from their potential breach. Generally, the ranking of

security and privacy targets is important, because companies need to be aware of their most important system weaknesses and prioritise security investments in those areas.

However, the judgement of the relative priority of privacy targets is a challenge. The extent of damage can often not be evaluated in terms of financial loss. In such cases, 'soft' factors must be considered, such as potential damage to a company's reputation or the social implications of a privacy breach for consumers. An informed qualitative assessment, conducted by experts, is often used to determine the degree of protection for each privacy target (see also [BSI2007] for different degrees of security protection of RFID systems).

Naturally, the degree of protection should be consistent with the negative consequences of a potential privacy breach. Such consequences can be anticipated for RFID operators and their customers (the 'data subjects'). Customers can lose social standing, money or even personal freedom as a result of a privacy breach. Regardless of whether this happens, companies can lose their reputation and damage their brand when privacy breaches become known to their customers or the public at large through negative press campaigns. RFID operators should therefore carefully consider how the breach of different privacy targets could impact their market reputation or lead to financial compensation payments. Based on this judgement, operators can prioritise privacy targets for their operations.

Operators can use Table 3 to identify the level of protection that is appropriate for typical damage scenarios. The table indicates which protection levels may be relevant and how a damage scenario might affect operators and data subjects. **The leading question is “What would happen if ...?”.**

Two perspectives should be considered: the perspective of the operator and the perspective of the data subject. The resulting judgements are combined, generating an overall score that assigns each privacy target to the “low – 1”, “medium – 2” or “high – 3” protection demand category. In a later state of the assessment, this category judgement helps operators to choose privacy controls that correspond in strength and vigour.

In Table 3, we use the legal term “data subject” to signal that both governmental institutions and private companies can be RFID operators that serve people in their roles as consumers or citizens.

Protection demand	Criteria for the assessment of protection demand					
	General description	Operator perspective		Data subject perspective		
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom
Low - 1	The impact of any loss or damage is limited and calculable.	Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.	The financial loss is acceptable to the organisation.	The processing of personal data could adversely affect the social standing of the data subject. The data subject's reputation is threatened for a short period of time.	The processing of personal data could adversely affect the financial well-being of the data subject.	The processing of personal data does not endanger the personal freedom of those concerned.
Medium - 2	The impact of any loss or damage is considerable.	Considerable impairment of the reputation / trustworthiness of the organisation can be expected.	The financial loss is considerable , but does not threaten the existence of the organisation.	The processing of personal data could have a seriously adverse effect on the social standing of the data subject. The data subject's reputation is threatened for a longer period of time.	The processing of personal data could have a seriously adverse effect on the financial well-being of the data subject.	The processing of personal data could endanger the personal freedom of those concerned.
High - 3	The impact of any loss or damage is devastating.	An international or nation-wide loss of reputation / trustworthiness is conceivable, possibly even endangering the existence of the organisation.	The financial loss threatens the existence of the organisation.	The processing of personal data could have a devastating effect on the social standing of the data subject. The data subject confronts a lasting loss of reputation.	The processing of personal data could have a devastating effect on the financial well-being of the data subject.	The processing of personal data could seriously endanger the personal freedom or result in the injury or death of the data subject.

Table 3: Protection demand categories

3.4 Step 4: Identification of Threats for each Privacy Target

After privacy targets have been identified, they can be used to systematically deduce threats. **The core question is how a privacy target is threatened.** For example, compliance with ensuring transparency (P1.1) may be threatened by incomplete or insufficient information describing the service (T1.1), or by information describing the service that is not current (T1.5). Again, keys are used to systematically link privacy targets to privacy threats. Annex III of the PIA Framework contains a relatively extensive but incomplete list of potential threats with RFID-specific examples. Depending on the industry and the RFID application, RFID operators can choose and comment on the potential threats from this list that are relevant to their operations. Alternatively, RFID operators may also need to add other threats that are more meaningful to them. Figure 4 uses keys to illustrate the link between privacy targets and threats.

Table 2

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name	
P1	Safeguarding quality of personal data	P1.1	Ensuring transparency
		P1.2	Providing purpose specification and limitation
		P1.3	Ensuring data avoidance and minimisation
		P1.4	Ensuring quality of data

Table 4

Threat code and name	Sub-threat code	Description of threat	Associated privacy target
T1 Lack of transparency – Missing or insufficient service information	T1.1	Incomplete or insufficient information describing the service. The operation details (data flows, data locations, ways of transmission, etc.) and the impacts of the RFID application are not sufficiently explained to the data subject.	P1.1
	T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	P1.1
	T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	P1.1 P1.2
	T1.4	Existing information describing the service is not easily understandable and / or special knowledge is needed to understand it, e.g. jurisdictional terminology, company-internal abbreviations, a distinct language, etc.	P1.1
	T1.5	Existing information describing the service is not kept up-to-date.	P1.1
	T1.6	Information provided in conjunction with an RFID emblem does not cover all areas and purposes for which RFID is used in a facility.	P1.1 P1.2

Figure 4: Systematically deriving privacy threats from privacy targets

The following table provides an extended list of threats that can be used to assess current and anticipated RFID service practices with respect to privacy and security targets. The given threats have been developed with the help of [EC1995], [ULD2010] and [BSI2005]. The threats are associated with the concrete privacy targets summarised in Table 2. RFID operators should be ready to adapt and extend this table to reflect their own situation.

The different threat sources are not listed in any order or hierarchical relationship in the table. They should be viewed as complementary elements.

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
T1	Lack of transparency – Missing or insufficient service information	T1.1	Incomplete or insufficient information describing the service. The operation details (data flows, data locations, ways of transmission, etc.) and the impacts of the RFID application are not sufficiently explained to the data subject. An RFID emblem is not displayed on the website of the RFID operator.	P1.1
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	P1.1
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	P1.1 P1.2
		T1.4	Existing information describing the service is not easily understandable and / or special knowledge is needed to understand it, e.g. jurisdictional terminology, company-internal abbreviations, a distinct language, etc.	P1.1
		T1.5	Existing information describing the service is not kept up-to-date.	P1.1
		T1.6	Information provided in conjunction with an RFID emblem does not cover all areas and purposes for which RFID is used in a facility.	P1.1 P1.2
	Lack of transparency – Missing or insufficient privacy statement	T1.7	No privacy statement is available.	P1.1
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	P1.1
		T1.9	The existing privacy statement does not provide contact information to reach the RFID Operator and does not provide contact details in case of questions or complaint.	P1.1
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	P1.1
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	P1.1 P4.1 P5.1

3 Privacy risk assessment methodology

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	P1.1
Lack of transparency- Missing RFID emblem		T1.13	At the entrance of a respective facility using RFID or in places where RFID readers are deployed, no RFID emblem notifies data subjects of the data collection process.	P1.1
		T1.14	No RFID emblem is displayed on the product and the product packaging.	P1.1
Unspecified and unlimited purpose		T1.15	The purpose of the data collection is not specified. It is not specified that the collected data is used only for a distinct purpose or service that is transparent to the data subject as well as to employees.	P1.2
		T1.16	The data collection purpose is not documented in an adequate way.	P1.2 P1.1
		T1.17	Data that is stored and processed only for a specific purpose is not marked and / or managed accordingly; e.g. with corresponding access rights.	P1.2
Collection and/or combination of data exceeding purpose		T1.18	Collected data is processed for purposes other than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	P1.3
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	P1.3
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	P1.3
		T1.21	There are no measures in place that ensure data-minimisation. Thus, there are no measures to ensure that only relevant data is processed and that it is not processed excessively in relation to the purpose.	P1.3
		T1.22	There are no measures in place that prevent the linking of data sets. Thus, data collected during the occurrence of the service can be combined with data acquired from a third party or with data from another service the operator / organisation is offering.	P1.3
		T1.23	There are no measures in place that prevent the reading and tracking of the tagged item through unauthorised parties. The RFID tag has no read protection.	P1.3
Missing quality assurance of data		T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	P1.4
		T1.25	The identification of the data subject is not conducted thoroughly.	P1.4

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
		T1.26	Procedures that regularly check (either by contacting the data subject or automatically searching publicly available data) that data is accurate and up-to-date have not been implemented.	P1.4
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	P1.4
	Unlimited data storage	T1.28	Data subjects' data as well as corresponding back-up data is not deleted or anonymised when it is no longer needed for the specified purpose. Erasure policies are missing.	P1.5
	T1.29	Data subjects' data, which is no longer needed for the specified purpose but cannot be deleted due to retention rules, cannot be excluded from regular data processing.	P1.5	
T2	Invalidation or non-existence of consent	T2.1	Consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	P2.1
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	P2.1
		T2.3	The relevant legal basis (e.g. consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.	P2.1
T3	Invalidation or non-existence of explicit consent when processing sensitive personal data	T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	P3.1
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	P3.1
		T3.3	The relevant legal basis (e.g. explicit consent, field of employment law, vital interests, not-for-profit-body, published sensitive data, defence of legal claims, special legal basis) has been transgressed.	P3.1
T4	No or insufficient information concerning collection of data from the data subject	T4.1	At the time of data collection, the data subject is not or not sufficiently informed about all of the following: <ul style="list-style-type: none"> - the identity of the data controller and of his representative if any, - the purpose of the processing, - the recipients of the data (is the data given to any third party?), - which questions on the registration form are voluntary and which are optional and what are the consequences when not replying, - the existence of the right of access to and the right to rectify the data concerning him. 	P4.1
		T4.2	The relevant information is not provided in an adequate form	P4.1

3 Privacy risk assessment methodology

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
	No or insufficient information concerning data that has not been obtained from the data subject		(e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	P4.1
		T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: <ul style="list-style-type: none"> - the identity of the data controller and of his representative if any, - the purpose of the processing, - the categories of data concerned, - the recipients of the data (is the data given to any third party?), - the existence of the right of access to and the right to rectify the data concerning him. 	P4.2
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	P4.2
		T4.6	The relevant information is not easily understandable; therefore, it is possible that the data subject will not be able to understand that the operator obtained information about him or her from a third party.	P4.2
T5	Inability to provide individualised information about processed data and purpose	T5.1	At the time of processing, the operator does not provide any interface to the data subject that the subject can use to efficiently identify what data about him or her is processed and what the data is used for. Even if the data subject sends a request requiring information, there is no procedure to automatically obtain this individualised information from the operator's systems.	P5.1
		T5.2	Access is possible but not to all relevant data, including: <ul style="list-style-type: none"> - confirmation as to whether or not data relating to the data subject is being processed, - the purpose of the processing, - the categories of data concerned, - the recipients or categories of recipients to whom the data is disclosed, - the data undergoing processing and any information as to the data's source, - the logic involved in any automatic processing of data and automated decisions. 	P5.1
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	P5.1

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
	Inability to rectify, erase or block individual data	T5.4	Successful access as well as subsequent data disclosure is not logged.	P5.1
		T5.5	A procedure (technical means and / or processes) that allows the data subject to rectify, erase or block individual data has not been implemented.	P5.2
		T5.6	Errors are not automatically rectified.	P5.2
		T5.7	There is no procedure that allows the erasure of individual data in back-up data.	P5.2
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	P5.2
		T5.9	Successful rectification, erasure and blocking is not logged.	P5.2
	Inability to notify third parties about rectification, erasure and blocking of individual data	T5.10	The operator has not implemented any procedure that would notify relevant third parties when individual data has been rectified, erased or blocked.	P5.3
T6	Inability to allow objection to the processing of personal data	T6.1	The data subject is not informed about the disclosure of his data to third parties or about the use of his data for direct marketing purposes and thus the data subject cannot object.	P6.1
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	P6.1
		T6.3	The operator has not implemented any procedure that would notify relevant third parties when a data subject has objected to the processing of his personal data.	P6.1
	Inability to allow objection to being subject to decisions that are solely based on automated processing of data	T6.4	The data subject cannot object to automated decision procedures that are used in the realm of the offered service.	P6.2
T7	Refer to security-relevant threats that are defined in BSI's technical guidelines TG 03126.	T7.1	Refer to the description of security-relevant threats that are defined in BSI's technical guidelines TG 03126.	P7.1

Table 4: Threats

Not all threats given as examples in the PIA Framework Annex III or in Table 4 may be equally probable. Many of them will not materialise at all from a specific operator’s perspective. An RFID operator must therefore identify those threats that are *likely* to occur in their organisation.

Threats can occur from within and outside of a particular system, and may derive from likely uses and possible misuses of the information. **As part of a full-scale PIA, a stakeholder group would typically identify threats and determine the likelihood of those threats.** The stakeholder group should include the technical staff responsible for the RFID roll-out, managers who will benefit from RFID data, those responsible for data protection of the respective RFID operator (if there is one) and end users of the RFID service. When stakeholders discuss each privacy target, they may identify additional threats that are relevant to the RFID application and processes. These additional threats, along with the associated privacy targets, need to be added to the table.

Based on the threat identification and assessment, each threat should be categorised as either “likely – yes” or “not likely – no”. Only threats that are likely to occur will later be mitigated.

Non-compliance through a lack of notification / reporting

In addition to application-related threats, RFID operators should also be aware of their reporting duties if they process personal data in the context of their RFID application. The “PIA Report [shall be made] available to the competent authorities at least six weeks before deployment” ([EC2011], p. 4). In most cases, a company’s data protection official or the department responsible for the RFID deployment will prepare the PIA report for the authorities.

That said, additional notification requirements are specified in Section IX of the EU Data Protection Directive; if RFID operators process personal data, they must consider these requirements. The requirements are summarised in Table 5.

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
T8	Non-compliance with notification requirements	T8.1	The operator does not notify the supervisory authority or the internal data protection officer as legally defined before carrying out personal data processing.	P8.1
		T8.2	The operator does not provide all the legally defined contents in his notification to the supervisory authority or the internal data protection officer.	P8.1
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	P8.1
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	P8.1

Table 5: Threats to notification requirements

3.5 Step 5: Identification and Recommendation of Controls Suited to Protect against Threats

The crucial step in the privacy risk assessment process is to identify controls that can help to “minimise, mitigate or eliminate the identified privacy risks” ([EC2011], p. 10). First, controls are considered that are implemented already or available for implementation. Identifying these controls helps operators judge real threats and their likelihood. Then, operators can use the identified threats and their associated likelihood to determine which of the identified controls are relevant and must be implemented. Figure 5 illustrates this relationship.

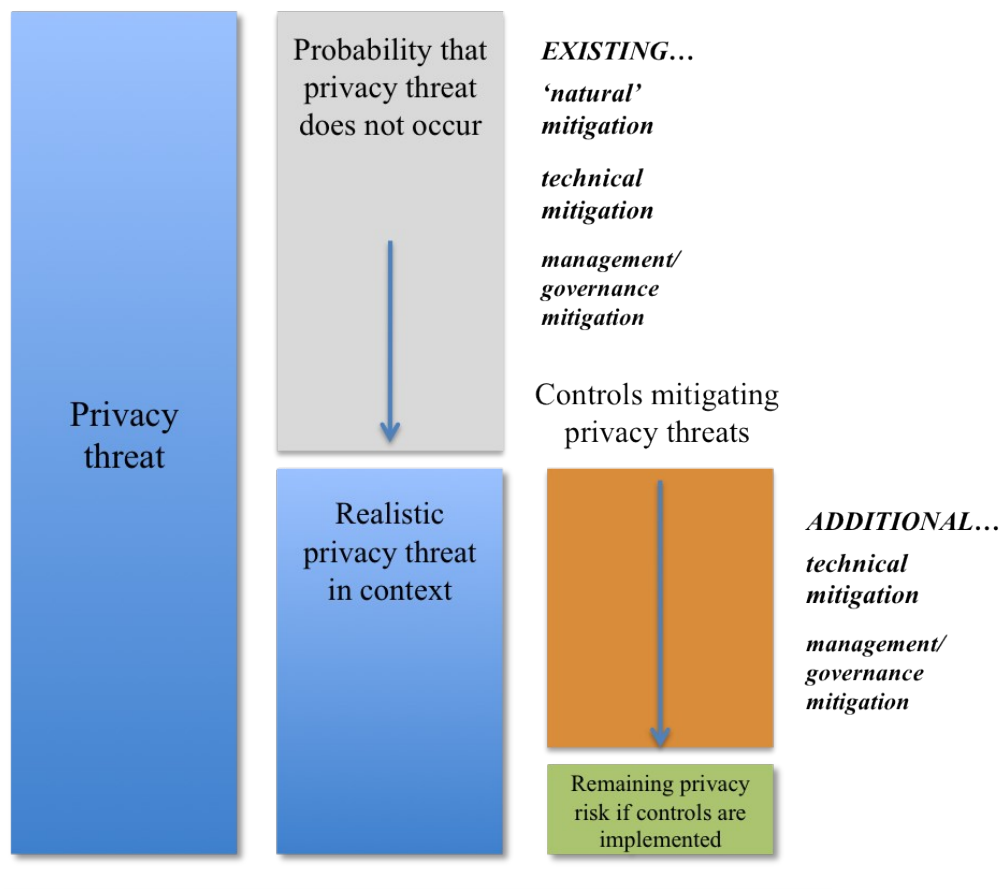


Figure 5: Assessing and controlling privacy risks

Controls are either of a technical or non-technical nature. Technical controls, such as access control mechanisms, authentication mechanisms and encryption methods, are directly incorporated into a system. Non-technical controls, on the other hand, are management and operational controls as well as accountability measures; these controls include policies or operational procedures and information measures taken with regard to data subjects. An exemplary list of both technical and policy controls for RFID is included in Annex IV of the PIA Framework. A much wider spectrum of concrete technical controls for RFID applications can be found in the sector-specific exemplary PIAs attached to this document and the German BSI's Technical Guidelines for Implementation and

Utilization of RFID-based Systems [BSI2007] (in particular, their different application areas on trade logistics [BSI2008], public transport [BSI2009] and employee cards [BSI2010]).

In general, technical controls can be categorised as either preventive or detective. Preventive controls inhibit violation attempts, while detective controls warn operators about violations or attempted violations. In the privacy context specifically, it is important to note a category of preventive 'natural' privacy controls created by the environment. Natural privacy controls are physical or social artefacts in the environment that enforce privacy-sensitive behaviour simply through the force of their existence. For example, if no readers that can conduct a tracking of items or individuals are physically installed (i.e. because there is no business case for them), then 'naturally' there is no (likely) threat to privacy through unauthorized readings.

At this point, it should be noted that the aim of the PIA Framework has been to encourage "Privacy-by-Design" (PbD) and thus the implementation of *technical* controls wherever feasible [EC2009]. As the EU Recommendation on the implementation of privacy and data protection principles in applications supported by RFID states: "...privacy and information security features should be built into RFID applications before their widespread use (principles of 'security and privacy-by-design')" ([EC2009], p.3). Consequently, the PIA Framework states as one of its explicit benefits that it fosters "privacy by design efforts at the early stages of the specification or development process" ([EC2011], p. 3).

One reason that the PIA Framework and the EU Recommendation target Privacy-by-Design through technical controls as an explicit goal is that EU privacy regulation implies considerable information duties for companies with regards to their customers. If companies want to process personal data, they need to get the consent of their customers. To remain legally compliant, companies need to intensively communicate with their customers about privacy issues. This communication is not desirable from a company's marketing perspective, nor is it appealing for customers, who incur considerable transaction cost. Privacy-by-Design therefore aims to minimise the creation of personal data in the first place through pre-emptive measures such as data minimisation, anonymisation of profiles and deletion rules (see the upper part of Table 6 for a structured overview). Companies that implement pre-emptive PbD measures consequently have much fewer reporting duties and can offer their customers a more seamless and less information-intensive service experience.

PbD also supports the need to ensure access control to and accountability for personal data. Here, authentication and authorization controls as well as logging measures (see Table 6) are vital. Such processes enforce a certain protection level and create transparency around personal data processing.

Privacy-by-Design Practices for RFID	Potential Measures of Privacy-by-Design for RFID		
	RFID tags	Operator back-end systems	Extended back-end systems (e.g. partner network)
Data-minimisation and -avoidance (e.g. through anonymisation, pseudonymisation, de-identification, deletion, unlinkability)	<ul style="list-style-type: none"> - avoiding the storage of additional unique identifiers on RFID tags - avoiding the storage of personal data on RFID tags 	<ul style="list-style-type: none"> - minimal granularity (e.g. limited time stamp and location information) - partial or no saving of complete unique identifiers (e.g. EPC serial number) - deletion of all data subjects' data as well as object data after a certain / specified period of time - specification and automated enforcement of deletion/erasure policies - implementation of anonymisation/pseudonymisation mechanisms - implementation of obfuscation mechanisms - limited linking of different data sets 	<ul style="list-style-type: none"> - no or limited sharing of RFID read data (e.g. EPCs read, time stamps, reader location IDs)
Access control (e.g. through identity management, authentication, authorisation)	<ul style="list-style-type: none"> - password protection of RFID tags' content - killing of RFID tags at store exits 	<ul style="list-style-type: none"> - rigorous and highly granular and restrictive management of access rights to RFID back end systems (e.g. EPCIS) 	<ul style="list-style-type: none"> - rigorous and highly granular and restrictive management of access rights to RFID back end systems (e.g. EPCIS)
Logging		<ul style="list-style-type: none"> - extensive logging of access to data - logging of system management operations (e.g. changes to access rights) 	<ul style="list-style-type: none"> - extensive logging of access to data as well as transfer of data - logging of network management operations (e.g. changes to access rights)

Table 6: Privacy-by-Design measures

If these technical privacy measures are not feasible for an RFID operator's application environment, business goals and personal data, the operator has to fulfil more extensive reporting duties.

The following table (Table 7) is intended as a guideline for which controls may be relevant. The table shows the threats that each control addresses. Each organisation must adapt and extend this table to reflect its situation.

3 Privacy risk assessment methodology

Control code	Level	Description of control	Addressed threat(s)
C1.1	General note	SERVICE DESCRIPTION	T1.1, T1.3, T1.4, T1.6
	low – 1	Rudimentary information describing the service is made available to the data subject.	
	medium – 2	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.	
	high – 3	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The technical functionality of the RFID technology is explained. Information about data processing, such as data flows, data location, and methods of transmission, is described in detail.	
C1.2	General note	INFORMATION ACCESSIBILITY	T1.2, T1.6
	low – 1	The information describing the service is made accessible at the operator's physical facilities. Thus, a data subject who visits the operator's facilities and asks for information can get information.	
	medium – 2	The information describing the service is made accessible at the operator's physical facilities and online.	
	high – 3	The information describing the service is proactively provided to the data subjects. It is made available in such a way that the data subject's attention is attracted. Online content is well-indexed and searchable.	
C1.3	General note	LANGUAGE/SEMANTICS OF INFORMATION	T1.4
	low – 1	The information describing the service is available in the language of the operator's home country and does not contain any expression requiring special knowledge (such as jurisdictional knowledge or company-internal terminology).	
	medium – 2	As in 1, plus: The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.	
	high – 3		
C1.4	General note	INFORMATION TIMELINESS	T1.5, T1.1
	low – 1	Each time there are changes to the service and the underlying application, the information describing the service is updated accordingly.	
	medium – 2	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.	
	high – 3		
C1.5	General note	PRIVACY STATEMENT	T1.7, T1.8, T1.9, T1.10, T1.11, T1.12
	low – 1	A comprehensive and complete privacy statement is made available to the data subject.	

Control code	Level	Description of control	Addressed threat(s)
	medium – 2	An extensive privacy statement that contains all required information in an easily understandable form is easily accessible, i.e. prominently linked from each web page of the operator.	
	high – 3	An extensive privacy statement that contains all required information in an easily understandable form is easily accessible, i.e. prominently linked from each web page of the operator. It is available in the most common languages.	
C1.6	General note	RFID EMBLEM	T1.13, T1.14
	low – 1	The RFID emblem is shown in such a way that it is clearly visible to every data subject entering the operator's facilities or being in read range. It is attached to all products and product packaging.	
	medium – 2	The RFID emblem is shown in such a way that it is clearly visible to every data subject entering the operator's facilities or being in read range. It is attached to all products and product packaging. Additionally, it is linked with informational material describing the service and the RFID technology.	
	high – 3		
C1.7	General note	PURPOSE SPECIFICATION	T1.15, T1.16
	low – 1	A purpose specification is available to the employees of the operator, to data subjects as well as to requesting authorities.	
	medium – 2	A purpose specification is available in two versions: a detailed version for the involved employees of the operator that includes system and application details and a version that is written for the data subjects. The latter one is easily accessible, e.g. on the operator's website.	
	high – 3	A purpose specification is available in two versions: a very detailed version for the involved employees of the operator that includes system and application details and a version that is written for the data subjects. The latter one is easily accessible, e.g. on the operator's website. The former one is regularly brought to the attention of the employees, e.g. during privacy training, to increase their awareness.	
C1.8	General note	ENSURING LIMITED DATA PROCESSING	T1.17, T1.18, T1.22
	low – 1	Employees are informed about the purpose of collected data and are asked to comply with the specified purpose.	
	medium – 2	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.	
	high – 3	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level.	
C1.9	General note	ENSURING PURPOSE RELATED PROCESSING	T1.18, T1.19
	low – 1	It is regularly checked that collected data is used only for the specified purpose. Corresponding access rights are regularly checked and updated.	
	medium – 2	It is regularly checked that collected data is used only for the specified purpose. Corresponding access rights are regularly checked and updated. Access to data and processing of data is logged on a level that is sufficient to detect potential misuse or processing for another purpose than the specified one.	
	high – 3		

3 Privacy risk assessment methodology

Control code	Level	Description of control	Addressed threat(s)
C1.10	General note	ENSURING DATA MINIMISATION	T1.20, T1.21
	low – 1	Data collection is regularly checked under the aspect of data minimisation (for technical control examples, see Table 6, e.g. storage avoidance, minimal granularity). Thus, it is regularly questioned whether only relevant data (relevant to the specified purpose) is collected from data subjects.	
	medium – 2		
	high – 3		
C1.11	General note	ENSURING TAG PROTECTION	T1.23
	low – 1	RFID tags are not secured. Stored information is difficult to interpret for third parties if they do not know the proprietary data format. The data subject gets information on how to get rid of / kill the tag.	
	medium – 2	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject.	
	high – 3	RFID tags are deactivated or killed by default before the data subject leaves the premises of the operator.	
C1.12	General note	ENSURING PERSONAL DATA QUALITY	T1.24
	low – 1	Data collection forms and tools are designed and implemented in such a way that completeness and correctness of the data collected from data subjects can be ensured in the best possible way.	
	medium – 2		
	high – 3		
C1.13	General note	ENSURING DATA SUBJECT AUTHENTICATION	T1.25, T5.3, T5.8
	low – 1	The data subject needs to identify or authenticate him or herself with his or her name and some security questions.	
	medium – 2	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.	
	high – 3		
C1.14	General note	ENSURING DATA ACCURACY	T1.26, T1.27
	low – 1	Processed data is regularly checked for accuracy and to ensure that it is up-to-date, e.g. on the basis of control samples of data subjects, either manually or automatically.	
	medium – 2		
	high – 3	Technical procedures are in place that automatically ensure that data is accurate and up-to-date, e.g. by searching through publicly available data or regularly asking all data subjects to check and rectify their data.	
C1.15	General note	ENABLING DATA DELETION	T1.28, T1.29

Control code	Level	Description of control	Addressed threat(s)
	low – 1	Data subjects' data that is no longer needed for the specified purpose is deleted or anonymised (for technical control examples, see Table 6). Legal retention requirements are considered.	
	medium – 2	Data subjects' data that is no longer needed for the specified purpose is deleted or anonymised (for technical control examples, see Table 6). Legal retention requirements are considered. Data that cannot be deleted due to retention rules is marked as such and excluded from regular data processing.	
	high – 3	Data subjects' data that is no longer needed for the specified purpose is deleted or anonymised (for technical control examples, see Table 6). Corresponding data in back-up systems is deleted, too. Legal retention requirements are considered. Data that cannot be deleted due to retention rules is marked as such and excluded from regular data processing.	
C2.1	General note	OBTAINING DATA SUBJECT'S CONSENT	T2.1, T2.2, T2.3
	low – 1	Legal personnel regularly checks if necessary consent is obtained at all and if it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms are checked by legal personnel.	
	medium – 2	Legal personnel regularly checks if necessary consent is obtained at all and if it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms are checked by legal personnel. Rules / policies concerning the legitimacy of processing personal data have been described and are available to all employees of the operator to give data subjects correct advice in situations where consent is gained.	
	high – 3	Legal personnel regularly checks if necessary consent is obtained at all and if it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms are checked by legal personnel. Rules / policies concerning the legitimacy of processing personal data have been described and are available to all employees of the operator to give data subjects correct advice in situations where consent is gained. Additionally, employees are taught about this subject during regular privacy training sessions to increase their awareness.	
C3.1	General note	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	T3.1, T3.2, T3.3
	low – 1	Legal personnel regularly check if necessary explicit consent is obtained at all and whether it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms and the like are checked by legal personnel.	
	medium – 2	Legal personnel regularly check if necessary explicit consent is obtained at all and whether it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms and the like are checked by legal personnel. Rules / policies concerning the legitimacy of processing sensitive personal data have been described and are available to all employees of the operator.	
	high – 3	Legal personnel regularly check if necessary explicit consent is obtained at all and whether it is obtained on the basis of complete or correct information and not upon an offer of advantage or threat of disadvantage. Consent forms and the like are checked by legal personnel. Rules / policies concerning the legitimacy of processing sensitive personal data have been described and are available to all employees of the operator. Additionally, employees are taught about this subject during regular privacy training sessions to increase their awareness.	
C4.1	General note	PROVIDING INFORMATION PROCESSING INFORMATION	T4.1, T4.2, T4.3
	low – 1	At the time of data collection, the data subject has access to information that describes all	

Control code	Level	Description of control	Addressed threat(s)
	medium – 2	relevant data: - the identity of the data controller and of his representative, if any, - the purpose of the processing, - the recipients of the data (is the data given to any third party?), - which questions on the registration form are voluntary and which are optional and what are the consequences of not replying, - the right to access and rectify the data about him. For example, this information might be accessible online via a link on the data collection form / tool and that leads to a separate web page that contains legal information.	
	high – 3	At the time of data collection, the data subject has access to information that describes all relevant data: - the identity of the data controller and of his representative if any, - the purpose of the processing, - the recipients of the data (is the data given to any third party?), - which questions on the registration form are voluntary and which are optional and what are the consequences of not replying, - the right to access and rectify the data about him. For example, this information is explicitly and easily understandable, and is presented and integrated into the data collection form or tool.	
C4.2	General note	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	T4.4, T4.5, T4.6
	low – 1	When data is obtained from a third party, the data subject has access to information that describes all relevant data:	
	medium – 2	- the identity of the data controller and of his representative, if any, - the purpose of the processing, - the categories of data concerned, - the recipients of the data (is the data given to any third party?), - the existence of the right of access to and the right to rectify the data concerning him. E.g. this information can be accessed online via a link that leads to a separate web page that contains a lot of legal information.	
	high – 3	When data is obtained from a third party, the data subject has access to information that describes all relevant data: - the identity of the data controller and of his representative if any, - the purpose of the processing, - the categories of data concerned,	

Control code	Level	Description of control	Addressed threat(s)
		<ul style="list-style-type: none"> - the recipients of the data (is the data given to any third party?), - the existence of the right of access to and the right to rectify the data concerning him. <p>E.g. this information is explicitly provided to him in an easily understandable way.</p>	
C5.1	General note	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	T5.1, T5.2
	low – 1	<p>A contact address is available that data subjects can use to ask about the purpose of their processed data or request other information. In particular:</p> <ul style="list-style-type: none"> - confirmation as to whether or not data relating to the data subject is being processed, - the purpose of the processing, - the categories of data concerned, - the recipients or categories of recipients to whom the data is disclosed, - the data undergoing processing and any information as to the data's source, - the logic involved in any automatic processing of data and automated decisions. <p>There are clearly defined processes that describe involved roles / employees, required actions and a time frame for answering a data subject's request for information. These requests are then individually processed and the required information / data is individually retrieved. Contact addresses of involved third parties are available to the data subject and he or she is asked to request information from these third parties him- or herself.</p>	
	medium – 2		
high – 3	<p>There is an application available to every data subject that enables him or her to efficiently get information about his or her processed data. In particular:</p> <ul style="list-style-type: none"> - confirmation as to whether or not data relating to the data subject is being processed, - the purpose of the processing, - the categories of data concerned, - the recipients or categories of recipients to whom the data is disclosed, - the data undergoing processing and any information as to the data's source, - the logic involved in any automatic processing of data and automated decisions. <p>Requests are automatically processed and individualised information is retrieved from the operator's systems.</p>		
C5.2	General note	LOGGING ACCESS TO PERSONAL DATA	T5.4, T5.9
	low – 1	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.	
	medium – 2		
high – 3			
C5.3	General note	HANDLING DATA SUBJECTS' CHANGE REQUESTS	T5.5, T5.6, T5.7, T5.10
	low – 1	A contact address is available that can be used by data subjects to ask for rectification, erasure or blocking of the processing of their personal data. There are clearly defined processes that describe involved roles / employees, required actions and a time frame for answering a data	
medium – 2			

3 Privacy risk assessment methodology

Control code	Level	Description of control	Addressed threat(s)
		subject's request. These requests are then individually processed and the respective data is individually rectified, erased or blocked. Contact addresses of involved third parties are available to the data subject and he is asked to request respective changes him- or herself.	
	high – 3	There is an application available to every data subject that enables him or her to efficiently request and conduct rectification, erasure or blocking of his or her processed data. Requests are automatically processed and individualised operations are performed in the operator's systems. In the case of data erasure, relevant data in backup systems is erased too. When data is changed that is relevant for third parties, a notification is sent out that describes the changes.	
C6.1	General note	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	T6.1, T6.2, T6.3
	low – 1	Notifications are sent to the data subject whenever the operator plans to disclose her personal data to third parties or to use data for a purpose that has not been explicitly stated before, such as for direct marketing. Objections are then individually processed. Contact addresses of involved third parties are available to the data subject and he or she is asked to direct objections to these third parties himself.	
	medium – 2		
	high – 3	Notifications are sent to the data subject whenever the operator plans to disclose data to third parties or to use data for a purpose that has not been explicitly stated before, such as for direct marketing. There is an application available to every data subject that enables him or her to efficiently create objections. Requests are automatically processed and individualised operations are performed in the operator's systems. In the case of involved third parties a notification is sent out to relevant third parties.	
C6.2	General note	HANDLING OBJECTIONS TO AUTOMATED DECISIONS	T6.4, T1.1
	low – 1	The logic involved in any automatic processing of data and automated decisions is described and made available to the data subjects. They are informed of their right to object to this automated decision making. A contact address is given. They are informed that the automated decisions cannot be disabled and that they are free to deregister from the service.	
	medium – 2	The logic involved in any automatic processing of data and automated decisions is described and made available to the data subjects. They are informed of their right to object to this automated decision making. A contact address is given. Objections are individually processed and automated decisions are disabled on request.	
	high – 3	As in 2, plus: There is an application available to every data subject that enables him or her to access detailed information about the automated decision procedures that are used and to object to these or even alter / influence them. Objections are automatically processed and automated decisions are disabled.	
C7.1	General note	SECURITY CONTROLS	T7.1
	low – 1	See relevant controls from TG 03126.	
	medium – 2	See relevant controls from TG 03126.	
	high – 3	See relevant controls from TG 03126.	
C8.1	General note	NOTIFICATION OF AUTHORITY	T8.1, T8.2, T8.4
	low – 1	It is ensured that the supervisory authority is notified before going live with the RFID application and that this notification contains all required information about the personal data processing. In addition, the PIA report needs to be made available to the authorities at least 6	
	medium – 2		

Control code	Level	Description of control	Addressed threat(s)
	high – 3	weeks prior to the RFID application’s launch.	
C8.2	General note	PRIOR CHECKING	T8.3
	low – 1	It is ensured that the legally required checking of the RFID application is executed by expert personnel.	
	medium – 2		
	high – 3		

Table 7: Controls

Only some of these controls will be relevant to a particular RFID application and the corresponding business processes. Which controls are relevant depends on the threats that were identified. Discussing all threats relevant to one's respective organisation may lead to the identification of additional controls that are relevant to the application and processes at hand. These additional controls need to be added to the table and linked to the identified threats.

Finally, operators should choose levels of controls that match the previously identified levels of protection demands, importance and likelihood of threats. For example, high protection demands combined with highly relevant threats should be mitigated with highly effective controls.

3.6 Step 6: Assessment and Documentation of Residual Risks

In step 6, the list of recommended controls that results from step 5 are evaluated. Recommended controls can be evaluated in terms of feasibility and effectiveness or by using a cost-benefit analysis. After the controls are evaluated, they can be sorted into a prioritised list. The result is a control implementation plan, from which residual risks are derived. Residual risks remain, for example, if an implemented control reduces the magnitude of the impact of a threat but does not eliminate the threat completely for technical or business reasons.

4 Bibliography

- [ART2010] Article 29 Data Protection Working Party: Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. WP 175. 13 July 2010.
- [BSI2005] Federal Office for Information Security (BSI): IT-Grundschutz Catalogues: Layer 1 – B1.5 Data protection. 2005.
- [BSI2007] Bartels, C., Kelter, H.: Technical Guidelines for Implementation and Utilisation of RFID-based Systems. ISSE/SECURE2007, Securing Electronic Business Processes, Vieweg-Verlag 2007, ISBN 978-3-8348-0346-7.
- [BSI2008] Federal Office for Information Security (BSI): TG 03126 - Technical Guidelines for the Secure Use of RFID. TG 03126-4 Application area “trade logistics”. 2008.
- [BSI2009] Federal Office for Information Security (BSI): TG 03126 - Technical Guidelines for the Secure Use of RFID. TG 03126-1 Application area “eTicketing in public transport”. 2009.
- [BSI2010] Federal Office for Information Security (BSI): Technical Guideline TR-03126-5. Technical Guidelines for the Secure Use of RFID (TG RFID). Subdocument 5: Application area “Electronic Employee ID Card”. Version 1.0, 2010.
- [EC1995] European Parliament and the Council (EC): 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. 24 October 1995, Art. 2(a).
- [EC2009] Commission of the European Communities (EC): Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Brussels, 2009.
- [EC2011] European Commission (EC): Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12 January 2011.
- [ENISA2010] European Network and Information Security Agency (ENISA), Emerging and Future Risks Framework – Introductory Manual, Heraklion, 2010.
- [ICO2009] [UK] Information Commissioners Office (ICO): Privacy Impact Assessment Handbook. Version 2.0, Wilmslow, Cheshire, June 2009.
- [ISO2008] International Organization for Standardization (ISO), ISO/IEC 27005 Information technology – Security techniques – Information Security Risk Management, Geneva, 2008.
- [NIST2002] National Institute for Standards and Technology (NIST): Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, July 2002.
- [SP2011] Spiekermann, S.: PIA II - A Proposal for a Privacy Impact Assessment Framework for RFID Applications. Vienna University of Economics and Business, 2011. (available at: http://cordis.europa.eu/fp7/ict/enet/policy_en.html, published there under the title: October 21th: German Industry Alternative Proposal on the RFID Privacy and Data Protection Impact Assessment Framework)

- [SPCR2009] Spiekermann, S., and Cranor, L. F.: Engineering Privacy. IEEE Transactions on Software Engineering, Vol. 35, No. 1, January/February 2009, pp. 67-82.
- [ULD2010] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): EuroPriSe Criteria. May 2010.