Bundesamt
für Sicherheit in der
Informationstechnik

Privacy Impact Assessment Guideline for RFID Applications

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

Contents

List of Figures

List of Tables

1 Privacy Impact Assessment Guideline

1.1 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 bodies[1] 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 1.2) explains who qualifies as an "RFID application operator" and what kind of responsibilities an operator has. Section 1.3 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. Chapters 2, 3 and 4 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).

1.2 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).

1.2.1 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

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 for conducting a PIA, becoming effectively the RFID operator. The 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.

1.2.2 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).

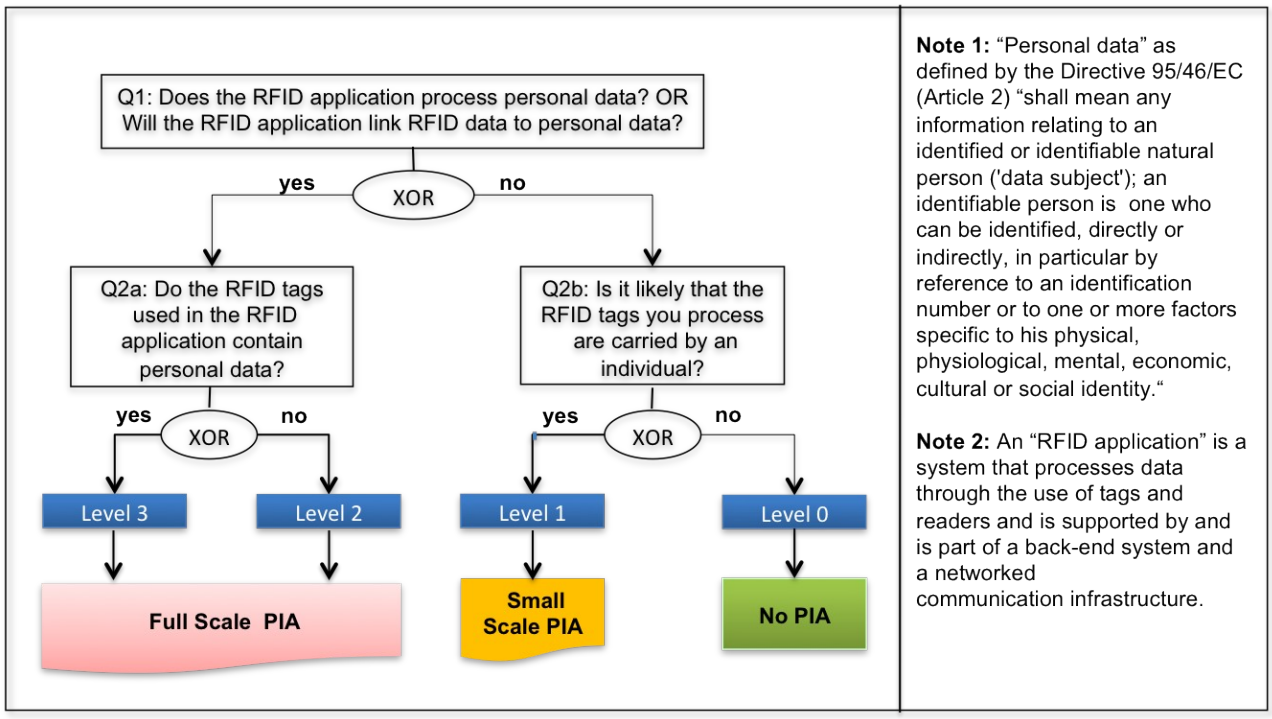

Figure 1: Decision tree for initial analysis (Source: [EC2011])

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.

1.2.3 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.

Report section	**Description**
RFID application operator	- 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	- 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	- Version number of PIA report (distinguishing new PIA or just minor changes) - Date of last change made to PIA report
RFID data processing	- List of types of data elements processed - Sensitive data processed?

Report section	Description
RFID data storage	- List of types of data elements stored - Storage duration
Internal RFID data transfer (if applicable)	- Description or diagrams of data flows of internal operations involving RFID data - Purpose(s) of transferring personal data
External RFID data transfer (if applicable)	- 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])

1.3 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.

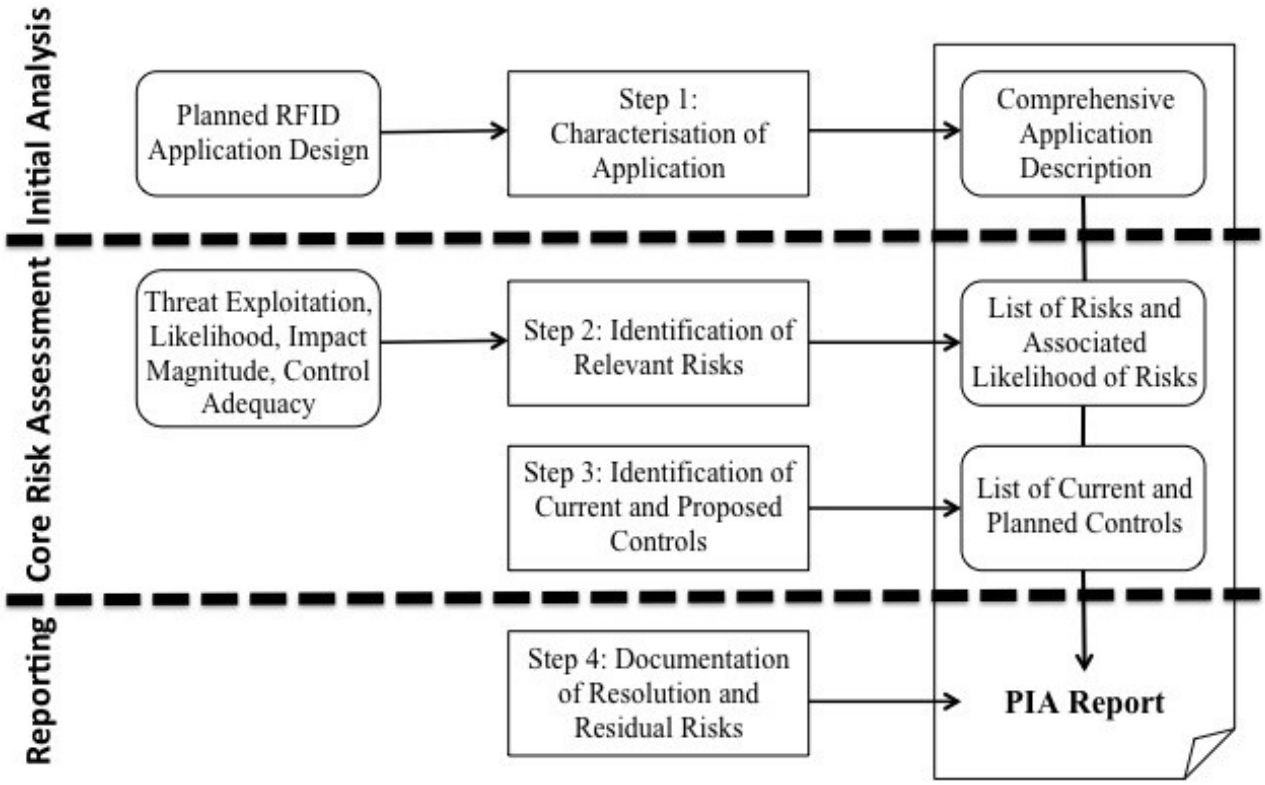

Figure 2: PIA process reference model

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 standards[5], 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,**

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

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.

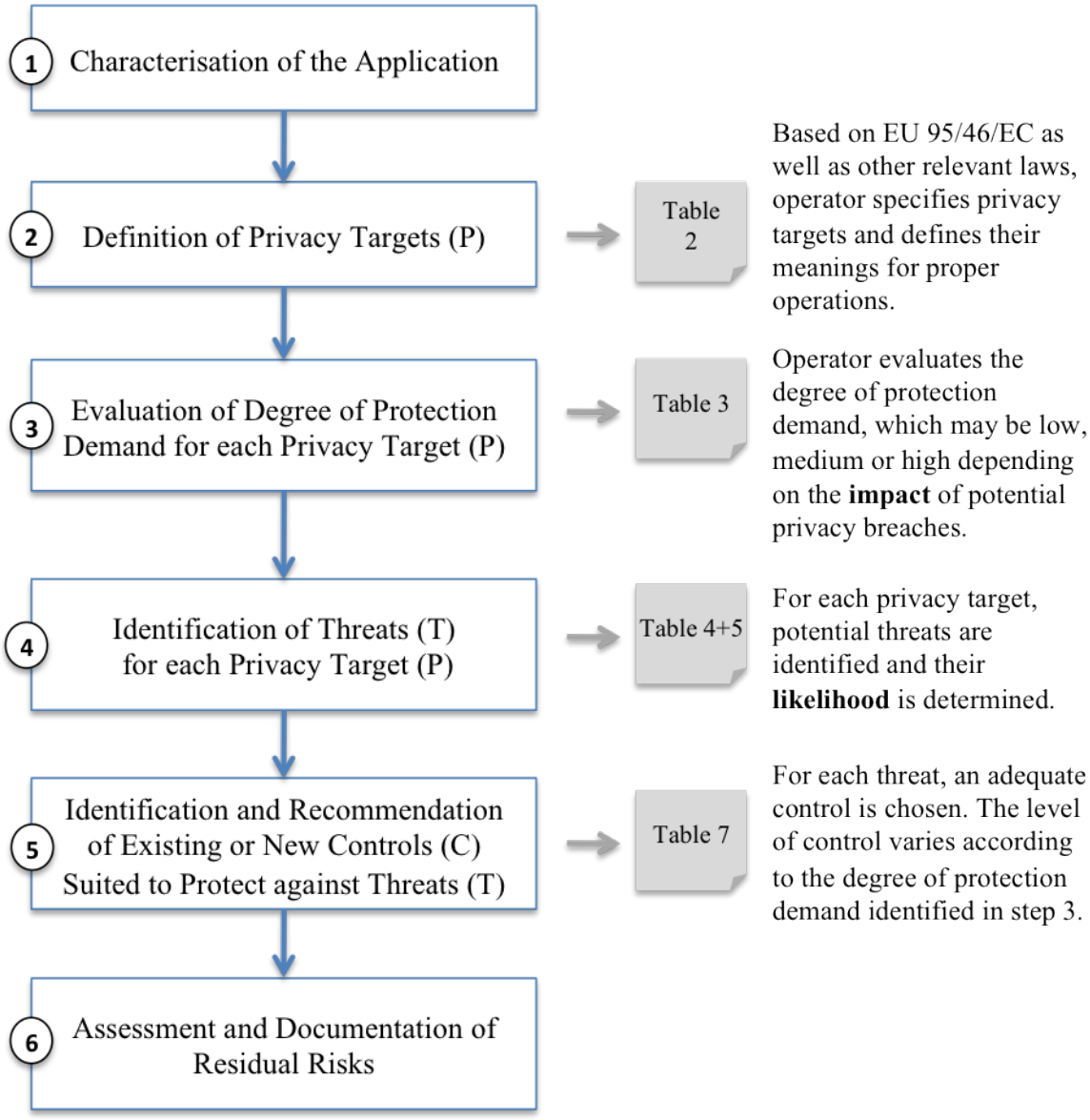

Figure 3: Privacy risk assessment methodology

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.

1.3.1 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.

1.3.2 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, … P*n.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]

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).

6 [BSI2007], [ENISA2010].

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name		Description of privacy target
		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).
		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).

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-á-vis an individual data subject.

Privacy targets as defined in the PIA Framework (Annex II)		Privacy target code and name		Description of privacy target
		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	***Here, security targets, which are defined in BSI's technical guidelines TG 03126, are relevant.*** 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

1.3.3 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

1.3.4 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
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	P1.1

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
	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
		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

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
		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: - 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 (e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	P4.1
		T4.3	The relevant information is not easily accessible but hidden	P4.1

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
			(e.g. small print in a legal section).	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: - 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: - 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
		T5.4	Successful access as well as subsequent data disclosure is not logged.	P5.1

Threat code and name		Sub-threat code	Description of threat	Associated privacy target
	Inability to rectify, erase or block individual data	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

1.3.5 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.

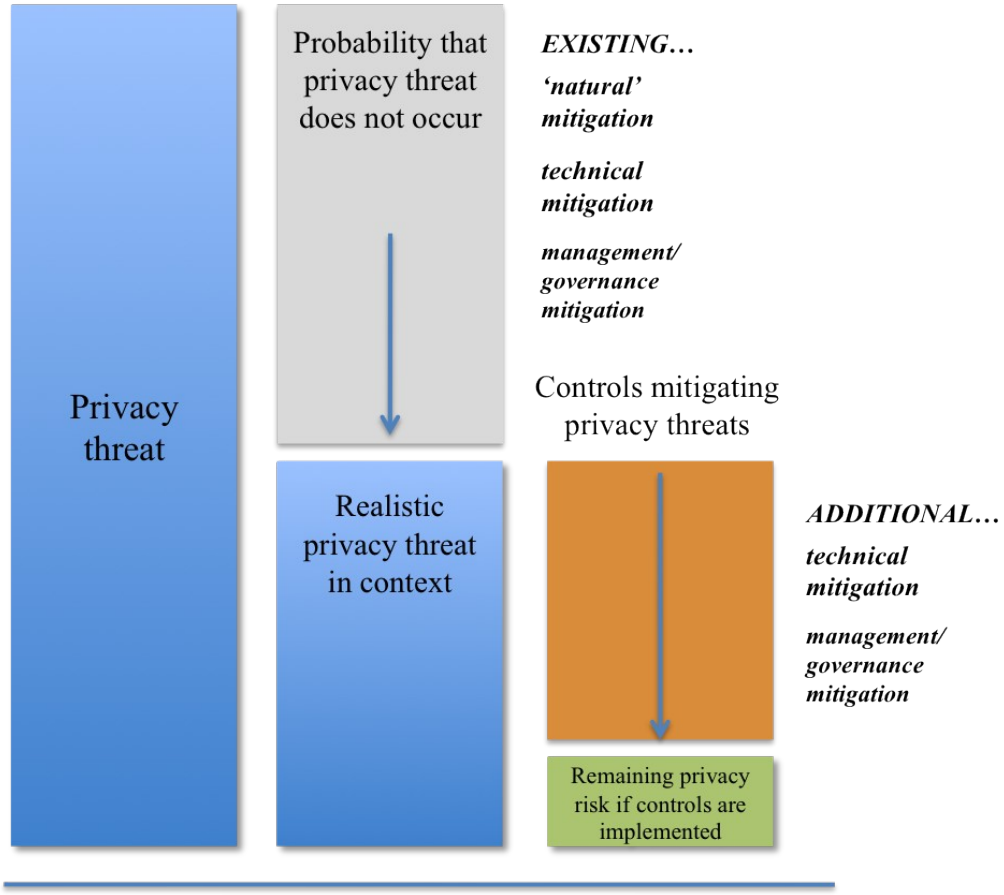

Figure 5: Assessing and controlling privacy risks

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 backend systems (e.g. partner network)**
Data-minimisation and -avoidance (e.g. through anonymisation, pseudonymisation, de-identification, deletion, unlinkability)	- avoiding the storage of additional unique identifiers on RFID tags - avoiding the storage of personal data on RFID tags	- 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	- no or limited sharing of RFID read data (e.g. EPCs read, time stamps, reader location IDs)

Privacy-by-Design	Potential Measures of Privacy-by-Design for RFID		
Practices for RFID **Access control** (e.g. through identity management, authentication, authorisation)	- password protection of RFID tags' content - killing of RFID tags at store exits	- rigorous and highly granular and restrictive management of access rights to RFID back end systems (e.g. EPCIS)	- rigorous and highly granular and restrictive management of access rights to RFID back end systems (e.g. EPCIS)
Logging		- extensive logging of access to data - logging of system management operations (e.g. changes to access rights)	- 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.

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

Control code	Level	Description of control	Addressed threat(s)
	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.	
	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	

Control code	Level	Description of control	Addressed threat(s)
		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		
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	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data.	
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	

Control code	Level	Description of control	Addressed threat(s)
	medium – 2	completeness and correctness of the data collected from data subjects can be ensured in the best possible way.	
	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
	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.	

Control code	Level	Description of control	Addressed threat(s)
		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 medium – 2	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 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

Control code	Level	Description of control	Addressed threat(s)
	low – 1 medium – 2	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, - 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, - 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 is explicitly provided to him in an easily understandable way.	
C5.1	General note	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	T5.1, T5.2
	low – 1 medium – 2	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: - 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. 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.	
	high – 3	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: - 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,	

Control code	Level	Description of control	Addressed threat(s)
		- 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. Requests are automatically processed and individualised information is retrieved from the operator's systems.	
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 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.	
	medium – 2		
	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	

Control code	Level	Description of control	Addressed threat(s)
		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 weeks prior to the RFID application's launch.	
	medium – 2		
	high – 3		
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.

1.3.6 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.

2 Retail Scenario

2.1 Initial analysis

For the initial analysis, the decision tree shown in Figure 1 is used. For the current scenario, the answer to Q1 is: Yes, the RFID application does process personal data. Personal data is stored and processed in consumer accounts in the customer relationship management system and in personalised user accounts and profiles in the shop-floor management system and added-value service management system.

The answer to Q2a is open to some interpretation: If the answer is based solely on the definition of personal data in the Directive 95/46/EC, RFID tags used in the application do not contain personal data. Consequently, the resulting level of PIA analysis is 2 and a full scale PIA is required. If, however, the answer to this question is based on the definition of personal data from Directive 95/46/EC **as well as** WP 136 [ART2007] and WP 175 [ART2010], then RFID tags used in the application do contain personal data. Personal data is involved in the loyalty card program and may also play a role for tagged products that are used by the consumer for added-value services. As a result, the retailer operating the current scenario is at level 3 of the PIA analysis and needs to conduct a full scale PIA.

Both answers to Q2a require a full scale PIA.

2.2 Risk assessment

The following description of a risk assessment is an exemplary execution of a PIA. A PIA that is conducted by a different group of stakeholders may lead to different conclusions. In particular, the context descriptions and examples in step 2, as well as the reasoning used to derive the demand categories in step 3, might be subjective and are a result of the discussions of the participating stakeholder group. Again, another stakeholder group may come up with different and additional damage scenarios and potential implications. The aim of a PIA is to create a common understanding about the RFID application's privacy implications within the involved stakeholder group and thus facilitates commonly accepted conclusions.

2.2.1 Step 1: Characterisation of the application

2.2.1.1 Systems and entities

2.2.1.1.1 Systems and system components

Figure 6 gives a generic overview regarding the systems and their associated components that form the backend system, which is required to realize the described retail scenario. Most likely, the different systems will reside on different locations and will be under the responsibility of different entities. This is indicated in Figure 6 by grouping the systems and their components accordingly.

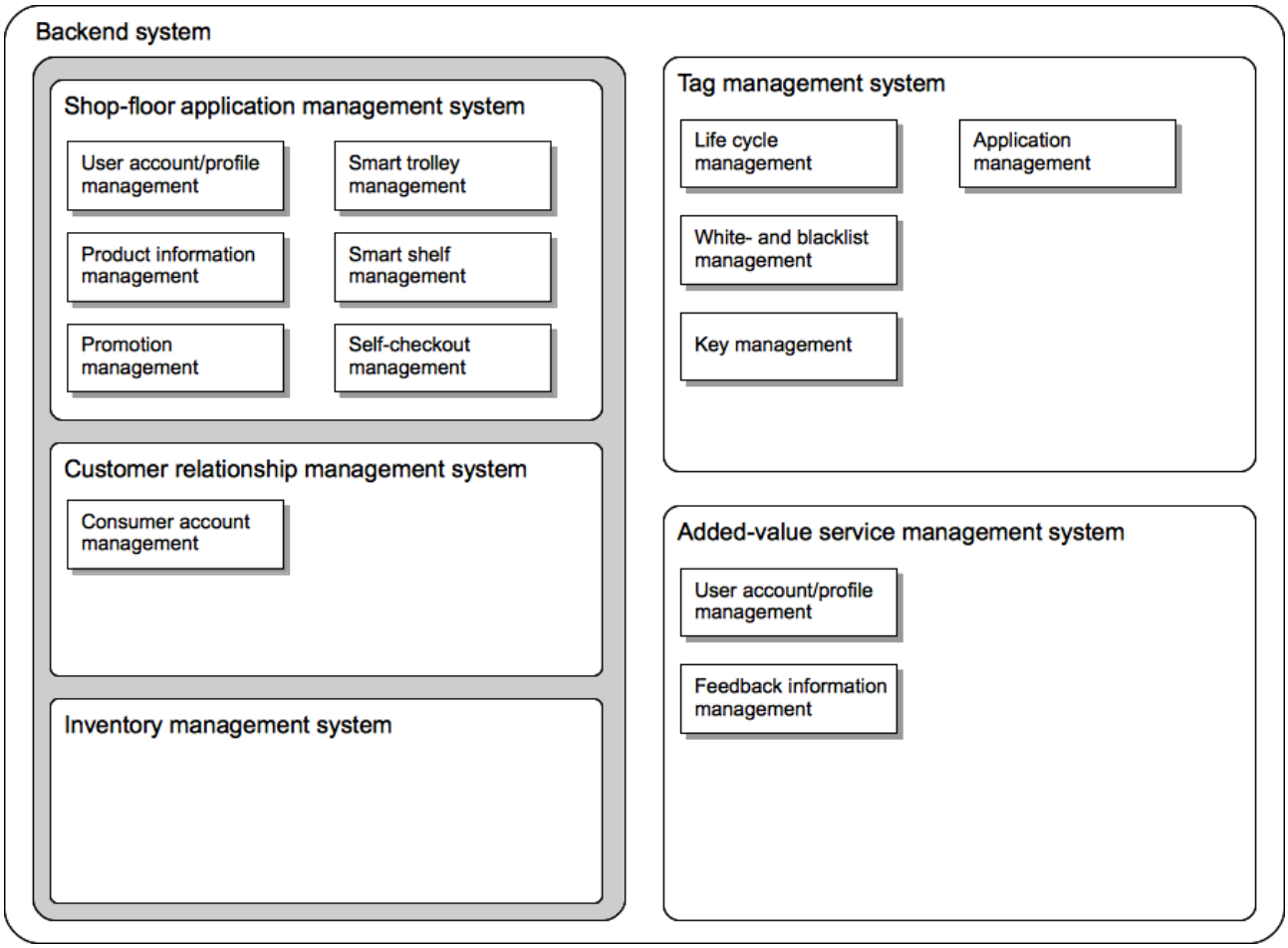

Figure 6: Retail backend system

The shop-floor application management system manages the single shop-floor applications as well as their interaction. It consists of the following six main components:

- User account/profile management
  This component provides all necessary functions to create, update and delete user accounts. These accounts may either be personalised, pseudonymous or anonymous.
  An account is *personalised* if a consumer decided to obtain a loyalty card, which is personalised in his name. Thus, the loyalty card is optically personalised with the consumer's name and the user account is directly linked with the consumer account in the CRM system. An account is *pseudonymous* if a consumer decided to obtain a loyalty card, which is personalized with a pseudonym. Thus, the loyalty card is either optically personalised with the pseudonym or not optically personalised at all. In this case, there is no link between the consumer's data in the CRM system and the user account data in the shop-floor management system. But there is a comprehensive user account, which contains all relevant data of the pseudonym.
  An account is *anonymous*, if no loyalty card is used by the consumer. This account contains all relevant data of one shopping visit on the shop floor. Thus, it is not a comprehensive one but it only reflects a consumer's behaviour concerning one single visit.
- Product information management
  This component provides all necessary functions to gather, structure, update and distribute detailed product information. Product information needs to be gathered from product manufacturers as well as from other information providers.

- Promotion management
  This component provides all necessary functions to gather, update and distribute promotion information. Promotion information might be static product ads, short films, promotional information, etc. Before distributing this information to the shop-floor applications, it needs to be coordinated with the inventory management system that respective products are on stock and thus available for the consumer.
- Smart trolley management
  This component provides all necessary functions to maintain the functionality of each smart trolley and to manage their whereabouts.
- Smart shelf management
  This component provides all necessary functions to aggregate inventory states from each smart shelf and to aggregate data about the promotional ads that have been shown on the integrated displays.
- Self-checkout management
  This component provides all necessary functions to steer the self-checkout process.

The customer relationship management system manages data of all the consumers, who participate in the loyalty program.

- Consumer account management
  This component provides all necessary functions to create, update and delete consumer accounts. These accounts contain personal data of consumers, e.g. name and address.

The inventory management system deals with the timely ordering of products, stock monitoring, supplier management and the like.

As there are different carrier mediums utilized throughout the described retail scenario, these are summarized under the term “tag”. In the detailed use case descriptions, the term “tag” is then specified with prefixes, e.g. product tag or loyalty card tag.

The tag management system provides the functions and processes that are needed to manage the tags regardless of the relevant carrier medium. It consists of four main components:

- Life cycle management
  This component provides all necessary functions to personalise, configure and change the tag with the contact-less interface.
- White- and blacklist management
  This component provides all necessary functions to provide, update and distribute white- and blacklists of tags as well as applications.
- Key Management
  This component encloses all relevant security parameters and cryptographic keys. Key management procedures work as described in 7.10 of [BSI2008].
- Application Management
  This component provides all necessary functionality to provide, update and withdraw applications.

The added-value service management system is operated by a service provider and deals with the provision of an added-value service. It consists of two main components:

- User account/profile management
  This component provides all necessary functions to create, update and delete user accounts.

These accounts may either be personalised or pseudonymous. An account is *personalised* if a consumer decided to register himself using his actual name, e.g. an email address that contains his name. An account is *pseudonymous* if a consumer decided to register himself using e.g. an email address that is not linked to his actual name and thus is pseudonymous.

- Feedback information management
  This component provides all necessary functions to manage feedback information which is characteristic for the added-value service and to personalise this feedback according to user account data.

2.2.1.1.2 Shop-floor applications

The described retail scenario consists of the following shop-floor applications:

- Loyalty card
  The loyalty card contains a tag and is either optically personalized with a consumer's name or a pseudonym. Thus, it is an ID card with a contact-less interface.
- Smart trolley
  The trolley is enhanced with a display, which is big enough for a consumer to read written text and to watch pictures. There is a reader attached to the trolley, so that a consumer can comfortably scan products. Finally the trolley itself is tagged, so that readers that are positioned throughout the shop floor can read the trolley's tag.
- Smart shelf
  The shelf is enhanced with one or several displays dependent on the size of the shelf. There are several readers attached to the shelf. They are allocated in such a way that they can take in all the products that reside on the shelf. Thus, the smart shelf can monitor its inventory.
- Self-checkout
  The conveyor belt of the checkout is enhanced with a reader that is capable of scanning in products that have been put on the belt one after another. Additionally, there is a terminal consisting of touchscreen and payment facilities, which allows a consumer to take decisions e.g. which tags should be killed and which should be kept alive as well as to fulfil a payment transaction.

2.2.1.1.3 Entities and their roles

The following entities have been identified to be relevant for the described retail scenario:

- Consumer
  A person who enters the shop floor. He might be the holder of a loyalty card. The consumer is identical to the one described in [BSI2008], page 40.
- User
  A person who uses the shop-floor applications.
- Retailer
  An organisation that manages the shop and provides shop-floor applications and products. The retailer is identical to the one described in [BSI2008], page 40.
- Added-value service provider
  An organisation that offers an added-value service for a product.

- Service provider for the life cycle management of tags
  An organisation that offers life cycle management services for tags (dependent on or independent of the carrier medium). This service provider differs from the “disposer” described in [BSI2008], page 41. The disposer only deals with the disposal of tags, whereas the service provider, which is used here, manages the entire life cycle of tags.

2.2.1.2 Generic business processes

2.2.1.2.1 Process R-P1: Registering for and obtaining a loyalty card

Retailers either offer their own loyalty programs to their consumers or they are a member of an alliance of retailers that offer a loyalty program, which is managed by a service provider. Consumers, who participate in the offered loyalty program, profit from special discounts, coupons and personalised communication.

In order to participate, consumers need to provide some personal information to the retailer. The amount of personal data they need to provide might differ and depends on the underlying loyalty program. After successful registration the consumer obtains a membership identification. This can either be a loyalty card or an application that is tied to the consumer's smart phone. In the present scenario, an RFID-enabled loyalty card has been chosen as membership identification. This card can either be personalised

- with the consumer's name
  In this case, the consumer's name is printed on the card and the card's technical ID is linked to the consumer's personal data. Thus, there is a direct link between the consumer account, which contains the consumer's personal data and is managed in the CRM system, and the user account, which contains the consumer's profile data, e.g. preferences, shopping behaviour, personalised discounts etc. and is managed in the shop-floor application management system.
- or with a pseudonym
  In this case, a pseudonym is printed on the card and the card's technical ID is not linked to the consumer's personal data. Thus, there is no direct link between the consumer account in the CRM system and the user account in the shop-floor application management system. The consumer account only contains an entry that a card has been given to the consumer, but not which one. The consumer's profile data is gathered and managed in the pseudonymous user account. Consequently, the consumer still receives personalised services on the shop floor, but only in connection with his loyalty card. E.g. there is no possibility for the retailer to send personalised ads to the consumer's home address.

If the consumer wants to quit his membership of the loyalty program, the retailer offers a de-registration service. The retailer asserts, that, when a certain period of time elapsed after the consumer has filed the de-registration request, the consumer's data will be deleted.

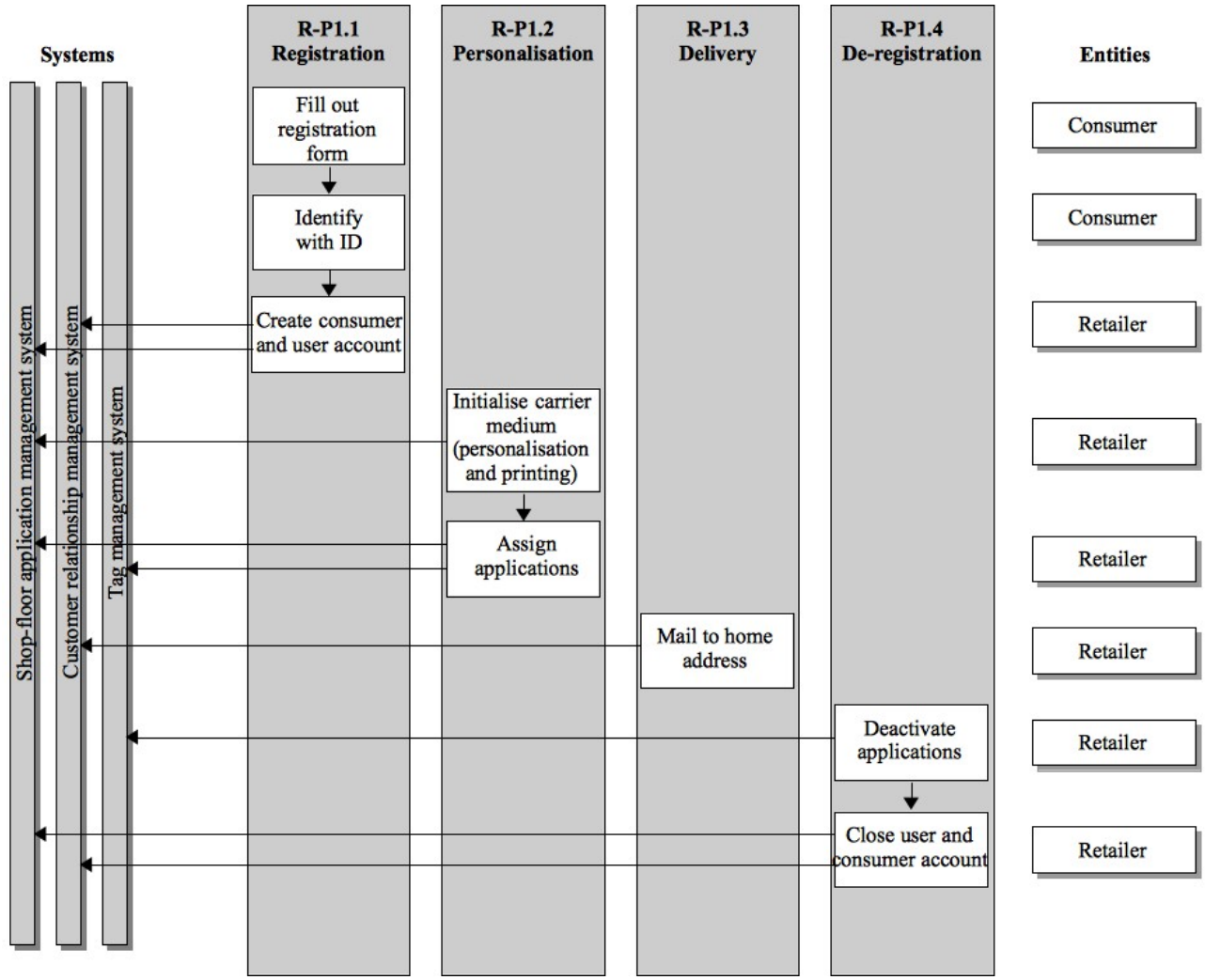

Figure 7: Process R-P1 – Registering for and obtaining a loyalty card

2.2.1.2.2 Process R-P2: Using a smart trolley

At the beginning of the shopping visit in the retail store, the consumer can either take out his loyalty card and authenticate to the smart trolley or he chooses to remain anonymous. When authenticated, the consumer can choose to use personalised shopping services that are offered by the retailer. Exemplary shopping services are:

- shopping list and navigation
  The consumer created a shopping list beforehand e.g. with the help of a web application and can access it on the smart trolley's display. The list is stored in the user account in the shop-floor application system. Additionally, the smart trolley can navigate him according to the shopping list through the store.
- allergy and/or intolerance support
  The consumer has entered his allergies and/or intolerances into his user account. When choosing a product helpful information is shown on the display. New products that might be interesting for the consumer's special condition are advertised on the display.

A service that is accessible for every consumer (authenticated and anonymous) is the generation of a list of the products the consumer chose to put into the trolley as well as the display of the current total price. A precondition for this service to work, is that the consumer holds to products to the reader that is attached to the smart trolley before putting them into the trolley.

With the help of the smart trolley the generation of consumer movement profiles is supported. Throughout the store several readers are positioned in such a way that they can register passing trolleys. These registered positions are then later assembled into movement profiles. These movement profiles are either stored in the user account of an authenticated consumer or in an anonymous user account. Later on, these movement profiles can then be aggregated in an anonymous form and an analysis can be performed.

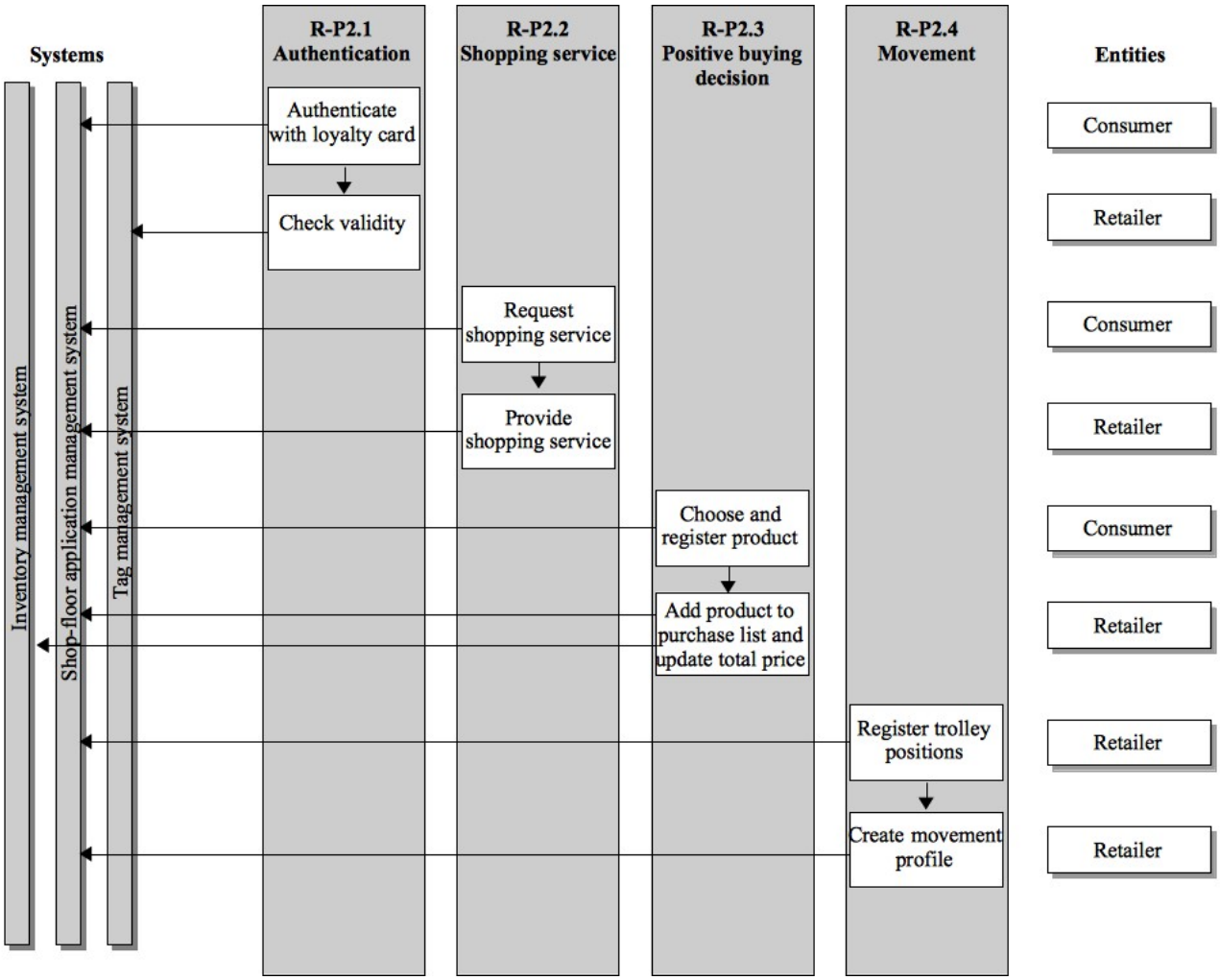

Figure 8: Process R-P2 – Using a smart trolley

2.2.1.2.3 Process R-P3: Using a smart shelf

When a consumer takes a product from the shelf to evaluate if he is going to buy it, product details or promotion information, which is connected to the product at hand, are displayed on the integrated screens. Before displaying any promotional information, the promotion management component of

the shop-floor application management system needs to check with the inventory system that the promoted products are actually on stock and available for the consumer.

As products that have been put back by a consumer are also registered by the smart shelf, there is the possibility to analyse whether displayed information had any effect on the purchase behaviour of the consumer. Thus, any event of displaying information is stored and can later be analysed in conjunction with the events of products put back on the shelf.

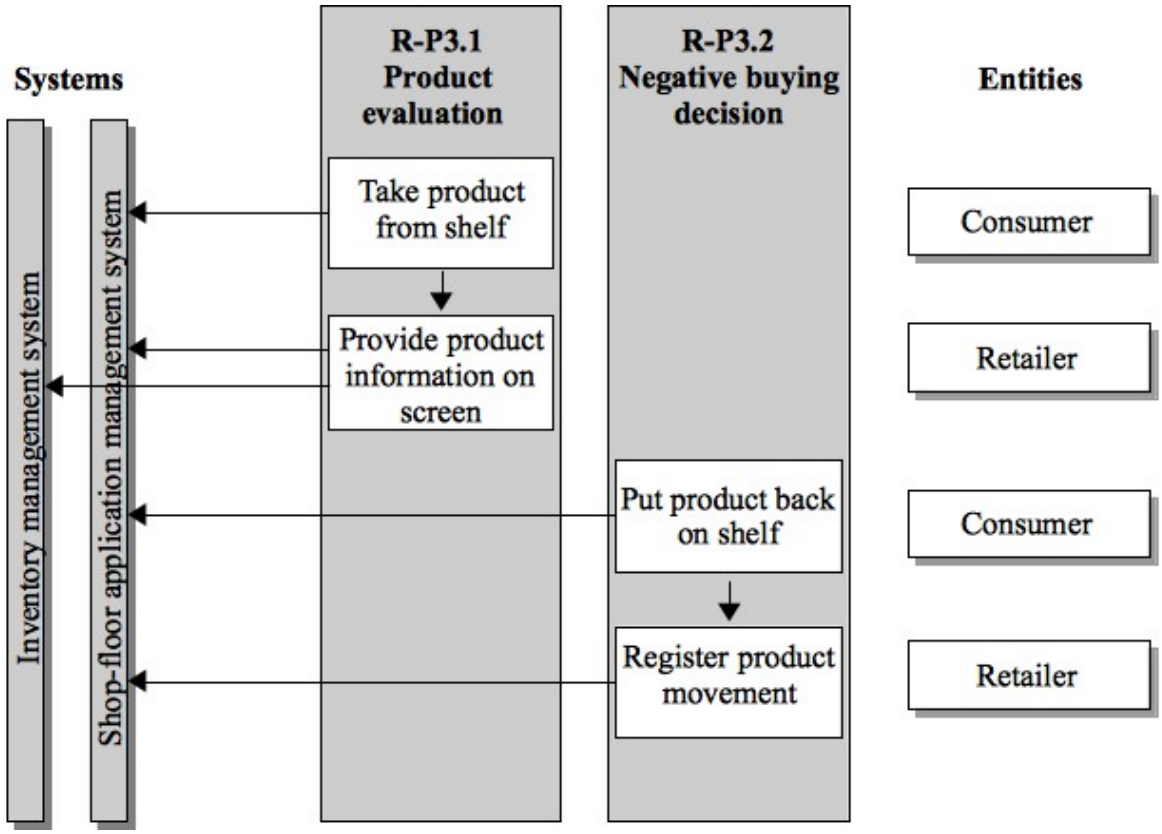

Figure 9: Process R-P3 – Using a smart shelf

2.2.1.2.4 Process R-P4: Using the self-checkout

The self-checkout offers consumers to choose whether product tags are killed, are put asleep or remain active. The following cases are conceivable:

- kill all tags
  The consumer has a trolley full of fast moving consumer goods, for which he does not need the tags to be active.
- kill some tags
  Next to some fast moving consumer goods, the consumer chose some expensive products, which come with added-value services he is determined to use. He will group the products on the conveyer belt in such a way that the tags of the fast moving consumer goods are killed and those of the expensive products remain active.
- put asleep some tags
  Similar to the case above, the consumer chose some expensive products. But he has not yet

decided whether to use the added-value services and he wants to control when and from whom these product tags are read. Thus he will group the products on the conveyor belt in such a way that the tags of the expensive products are put asleep.

The paying transaction itself can either be performed authenticated or anonymously. In the former case, the consumer provides his loyalty card to the reader of the self-checkout. When the payment transaction is finalised, the self-checkout informs the inventory management system about the products that have been purchased.

At the exit of the retail store some readers are installed to support the anti-theft strategy of the retailer. When a consumer leaves the store with his purchases, the product tags are read and checked against the information about outgoing products that resides in the inventory management system.

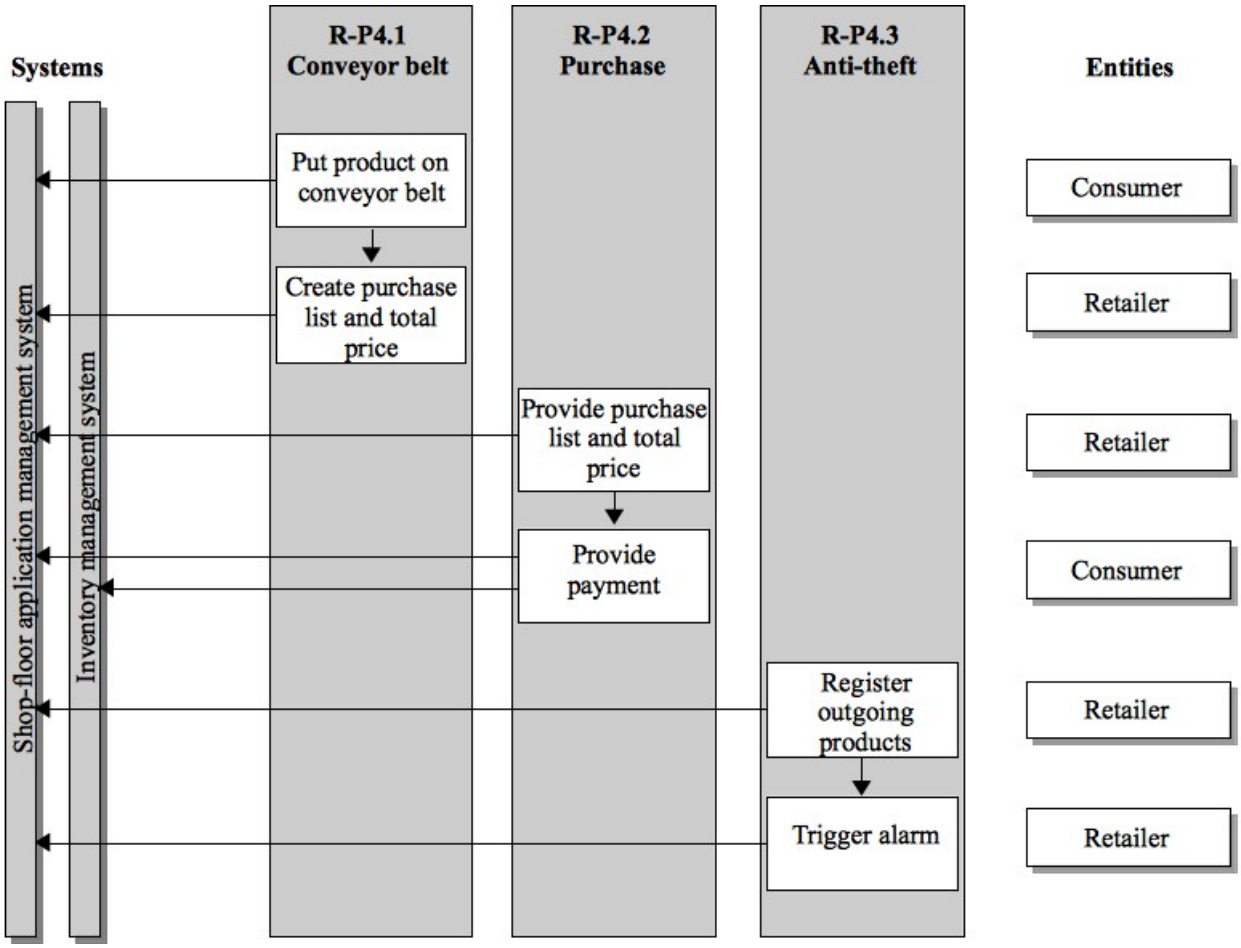

Figure 10: Process R-P4 – Using the self-checkout

2.2.1.2.5 Process R-P5: Registering for and using an added-value service

Some products might be enhanced with added-value services. These services can either be offered by a specialised service provider, by the manufacturer of the product or by the retailer.

An example would be a running shoe which contains a tag and separately provides a reader that can be connected to a handheld device. During usage the tag then continuously transmits data to the handheld device. Later on, the handheld device is connected to the Internet and the data is

transferred to a web application that is provided by the added-value service. In order to use this web application, the consumer first needs to register himself and create an account in the added-value service management system. In the simplest case, the provision of an email address might suffice to create such an account. Thus, a consumer can either provide an email address that contains his name and consequently directly links to his personal data or he provides a pseudonymous or even anonymous email address.

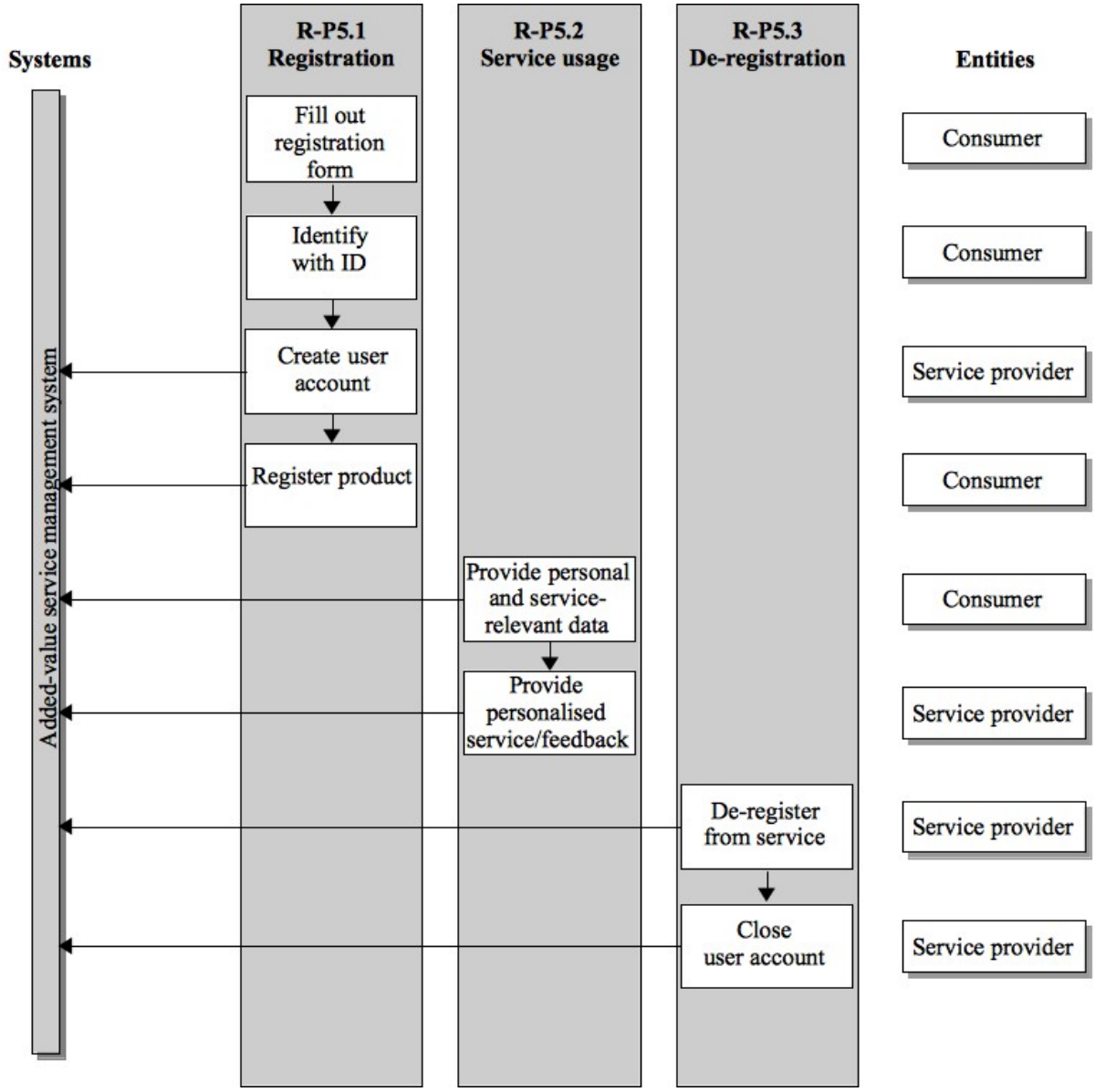

Figure 11: Process R-P5 – Registering for and using an added-value service

2.2.1.2.6 Process R-P6: Disposing a tagged product

In the case, that a product with a functioning tag reaches its end-of-life from the viewpoint of the owner/consumer, there is the need to either recycle this product and/or tag or to dispose it.

Recycling is only possible if the tag can be depersonalised and potentially re-personalised. A tag is personalised if one of its IDs is linked to personal data or if it contains personal data. As a consequence, to depersonalise a tag, it must be possible to break the link between IDs and personal data and/or to delete ID(s) and personal data from the tag.

Before disposing the tag, it can either be manually destroyed or the kill command can be executed.

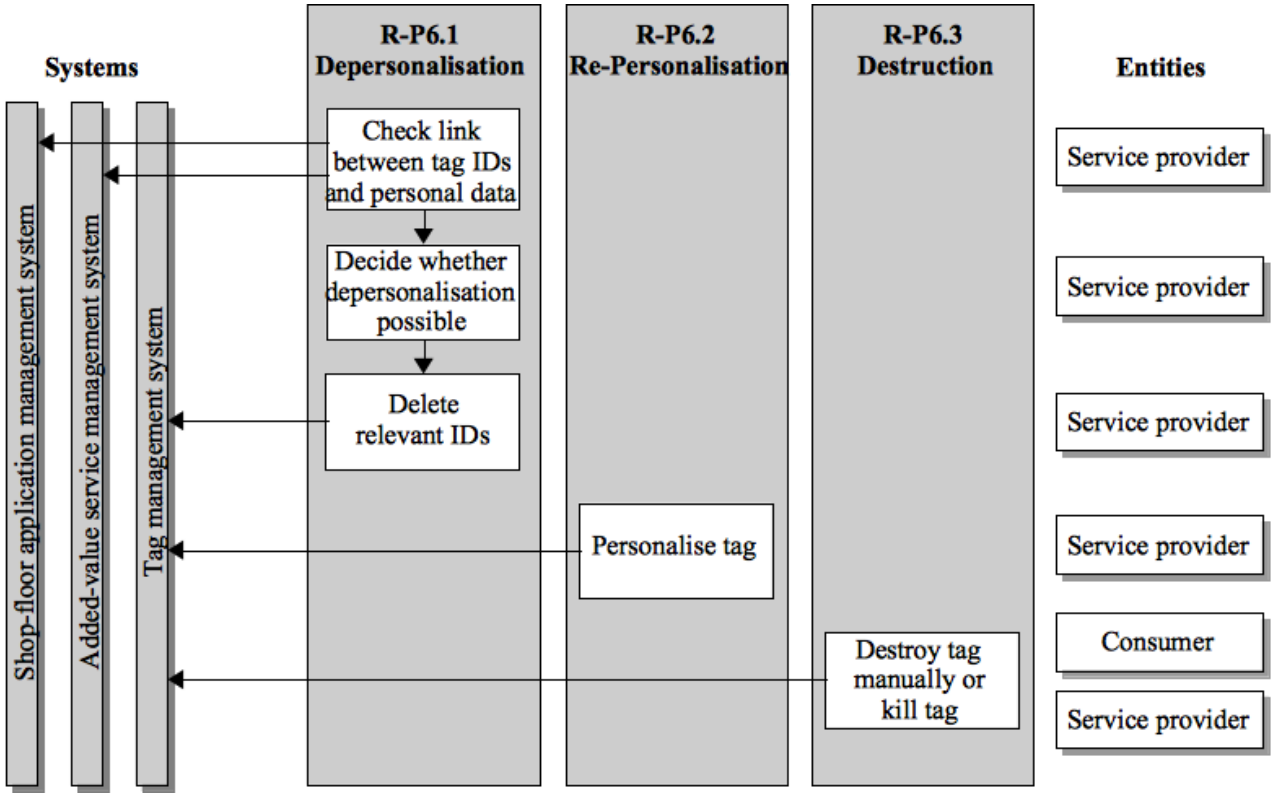

Figure 12: Process R-P6 – Disposing a tagged product

2.2.1.3 Use cases

2.2.1.3.1 Use case R-UC 1.1: Registering for the loyalty card program

The consumer needs to fill out a registration form to register for the loyalty card program. This can either be done

- via a piece of paper
  In this case, the service person who receives the paper form from the consumer checks if all personal data that is necessary to register has been provided by the consumer. Additionally, he checks the consumer's ID to ensure that the name on the form and the consumer are identical.
- or via a web application
  In this case, the application ensures that all necessary personal data has been provided by the consumer. The consumer proves his identity by providing his eID to the application.

The registration form is then processed and a consumer account containing the consumer's personal data is created in the CRM system. Furthermore, in the shop-floor application system a user account is created. If the consumer chose to register for a personalised membership, a direct link between consumer and user account is established. If the consumer chose to register for a pseudonymous membership, no such link is established, but the consumer account just holds the information that a loyalty card has been ordered for the consumer.

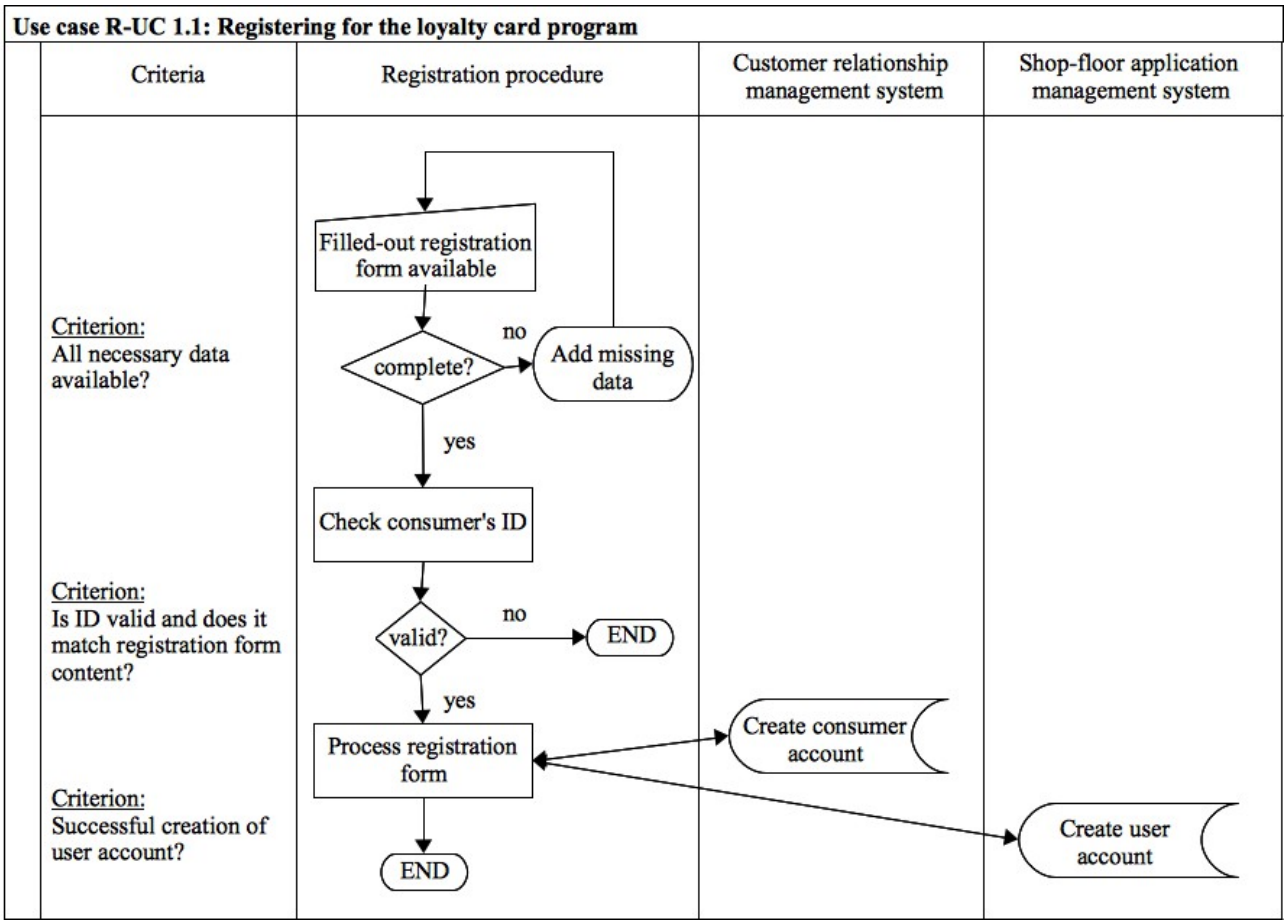

Figure 13: Use case R-UC 1.1 – Registering for the loyalty card program

2.2.1.3.2 Use case R-UC 1.2: Personalising the loyalty card

The order request for a loyalty card is processed by the tag management system. A new loyalty card is initialised with an ID and this ID is then registered in the respective user account. If the membership of the consumer encompasses the usage of distinct card applications, these are initialised and registered in the user account, too. Finally, the consumer's name or a pseudonym is printed onto the card.

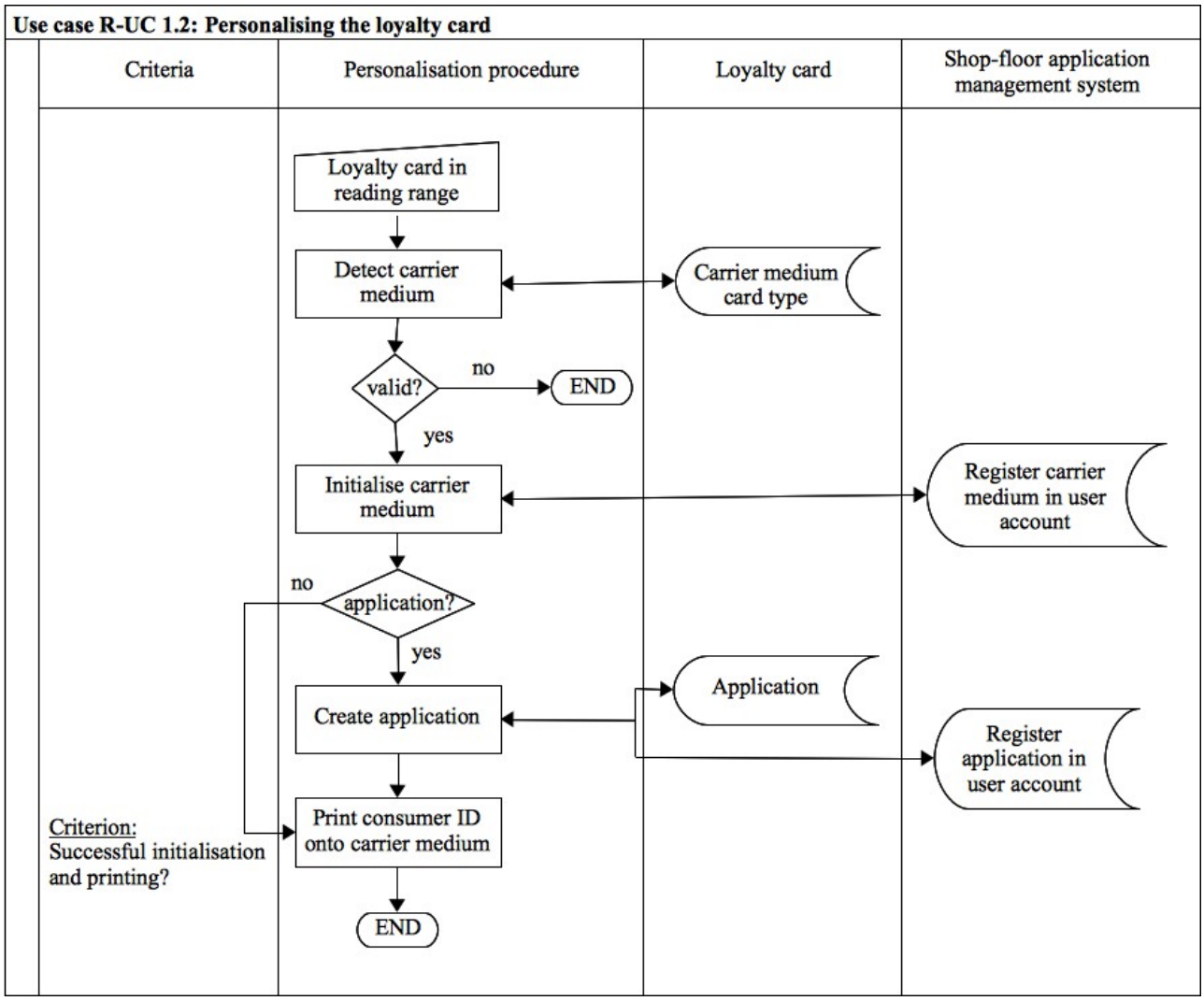

Figure 14: Use case R-UC 1.2 – Personalising the loyalty card

2.2.1.3.3 Use case R-UC 1.3: Delivering the personalised loyalty card

The personalised loyalty card is then either mailed to the consumer's home address or, especially in the case of a pseudonymous membership, the card can be fetched at the retailer's service point.

2.2.1.3.4 Use case R-UC 1.4: De-registering from the loyalty card program

The prerequisite for this use case is the application of a consumer for a de-registration. The de-registration request is only accepted and filed for further processing after positively identifying the consumer.

When a de-registration request has been filed, the respective data is retrieved from the user account. If there are any card applications registered in the user account, these are blocked and the application-specific black- and whitelists are updated accordingly. In the next step the loyalty card itself is blocked and the carrier medium-specific black- and whitelists are updated accordingly. Consequently, the consumer cannot use his loyalty card anymore.

But he might still be able to enter a retail web application e.g. with user name and password. Thus, the next step of the de-registration procedure is to add de-registration entries to the user and consumer account.

Finally, it needs to be checked whether the user account has to be deleted. If it does not contain any personal data or references to personal data its data could be saved by the retailer and further used for analysis purposes. If the user account contains personal data or the retailer does not want to keep the data, the deletion of the user and the consumer account is scheduled. Now starts a dedicated period of time during which the consumer can take back his de-registration request. Only when this period of time elapses, the actual deletion of consumer and user account is performed.

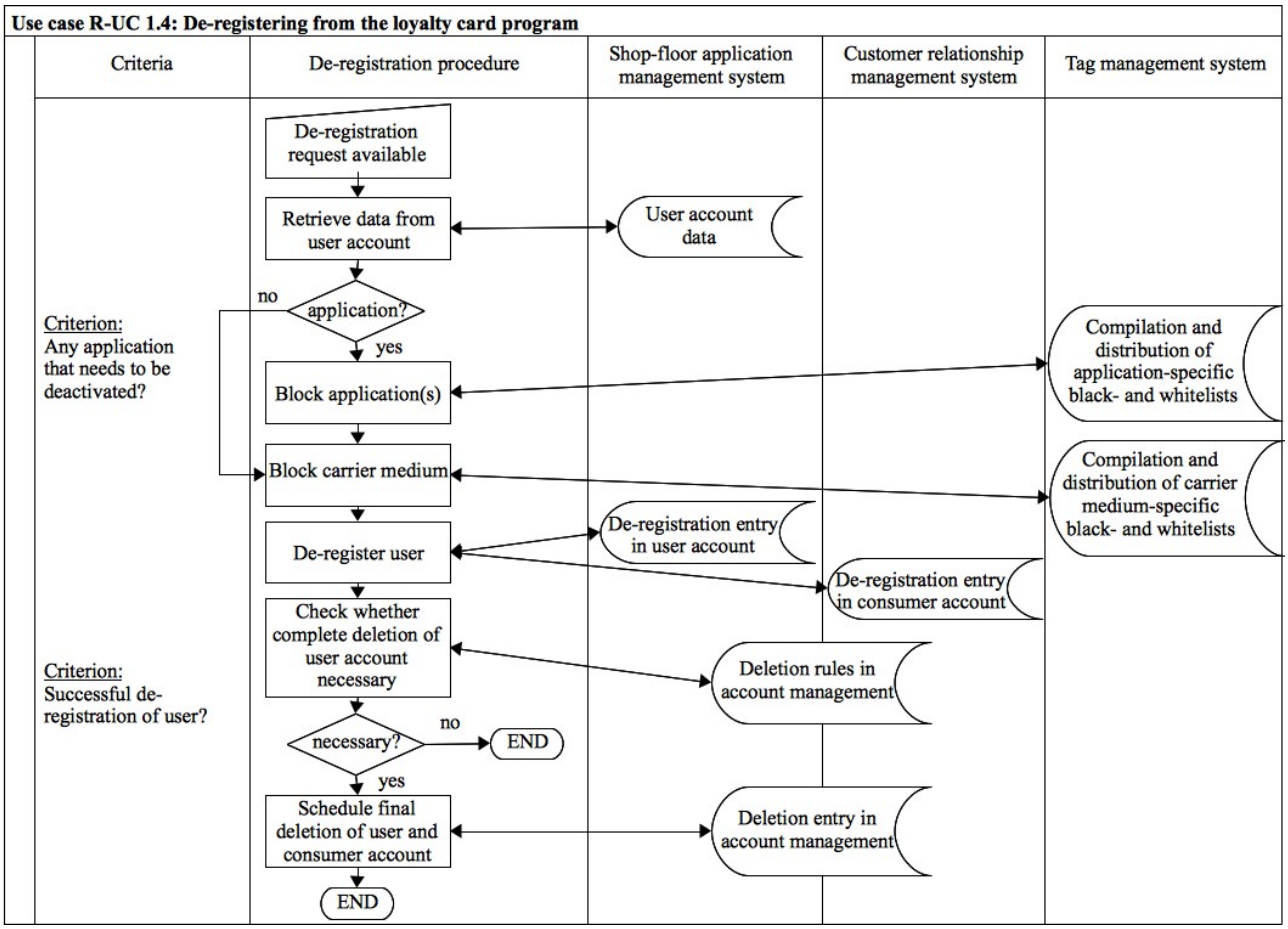

Figure 15: Use case R-UC 1.4 – De-registering from the loyalty card program

2.2.1.3.5 Use case R-UC 2.1: Authenticating with the loyalty card to the smart trolley

In order to authenticate to the smart trolley, the consumer needs to take out his loyalty card and hold it in front of the reader that is attached to the trolley. Access to the loyalty card might either be

- protected by an authentication factor
  In this case, the appropriate authentication factor, e.g. password, fingerprint, or the like, must be provided to the smart trolley's interface. It's correctness is then checked. If the authentication factor is correct, the authentication procedure continues. If it is not correct, an error message is displayed and the authentication procedure is aborted.

- or not
  In this case, it is enough to hold the loyalty card in front of the reader.

In the next step, the validity of the loyalty card itself is checked against the black- and whitelists that are provided by the tag management system. If the loyalty card is valid, the authentication procedure continues. If it is not valid, an error message is displayed and the authentication procedure is aborted.

Then some user date is retrieved from the user account, e.g. in order to show a personalised welcome message.

Finally, the authentication event itself is registered in the user account. The respective authentication entry contains the user's ID, the trolley ID and a timestamp.

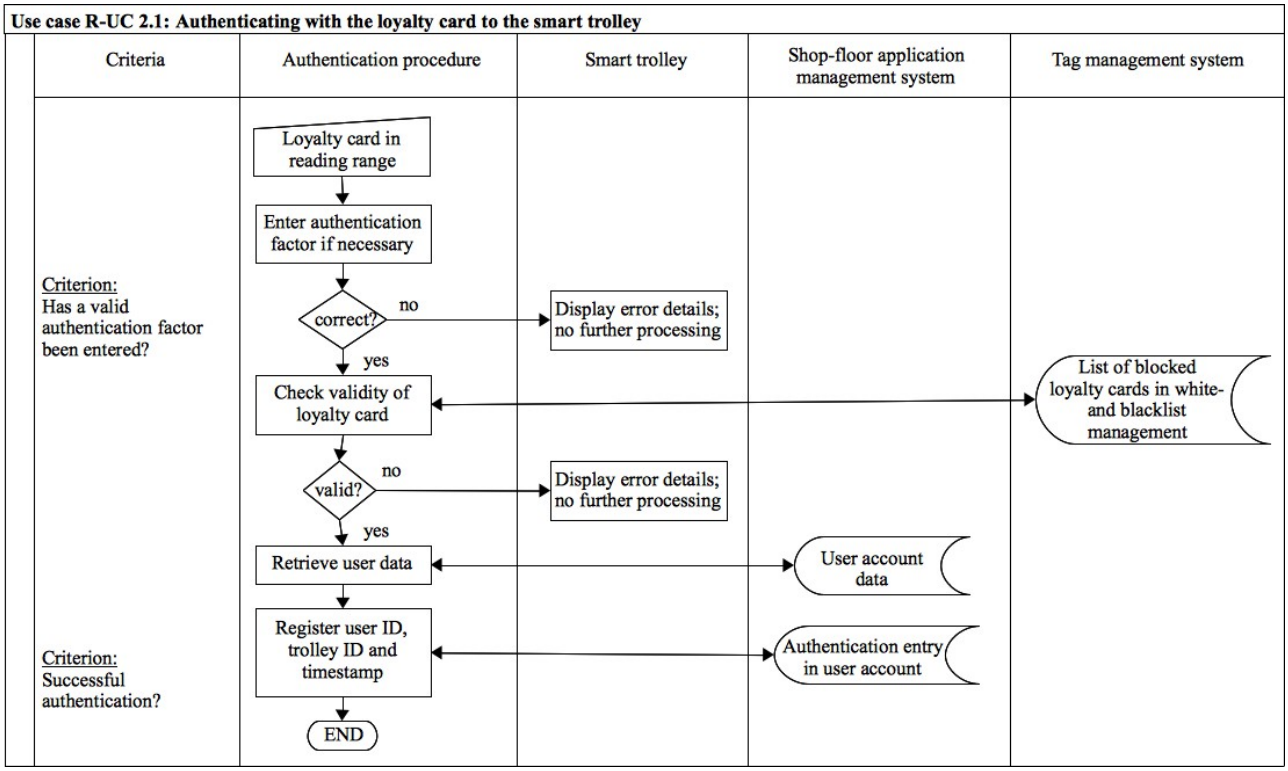

Figure 16: Use case R-UC 2.1 – Authenticating with the loyalty card to the smart trolley

2.2.1.3.6 Use case R-UC 2.2: Using shopping services

After successful authentication to the smart trolley, the consumer can now choose to use one of the shopping services that is offered to him. When the consumer requests the usage of shopping services, it is checked in the user account whether the consumer is allowed to use any services and whether these services are available at the given point in time. If this is not the case, an error message is displayed and the usage procedure is aborted. If there are some services available, these are displayed and the consumer can choose one of them.

The respective shopping service data is then retrieved. This data is either general service information or it is some personalised information, e.g. a shopping list, which is retrieved from the user's account.

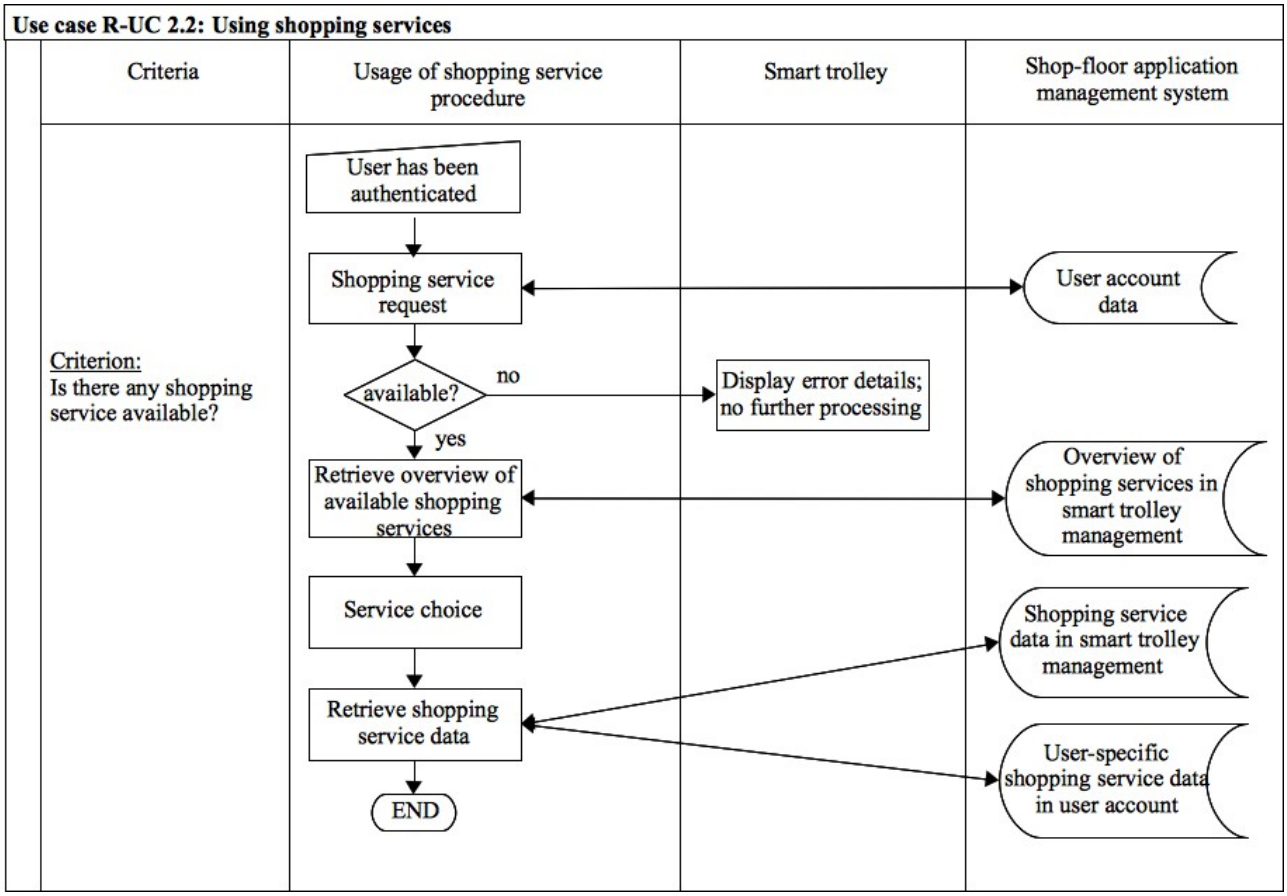

Figure 17: Use case R-UC 2.2 – Using shopping services

2.2.1.3.7 Use case R-UC 2.3a: Choosing a product and registering it with the smart trolley

When the consumer chooses to by a specific product and thus puts it into his trolley, he can hold it in front of the trolley's reader to get some more information on it and to add it to his purchase list.

The tag is read and if there is some product information available in the shop-floor application management system, detailed product information is retrieved and displayed. If no such information is available, an error message is displayed and the registering procedure is aborted.

Additionally, it is checked if some relevant promotion information is available. If this is the case and the corresponding product(s) is (are) available in the store according to the inventory management system, the respective ad(s) is displayed on the trolley's screen, too. Furthermore, it is checked whether the available product and/or promotion information can be personalised in any way consulting user account data, e.g. user preferences, ratings.

The product is then added to the purchase list and the total price of the products that have been put in the trolley is computed and displayed. An entry for adding the product to the purchase list is written into the user account.

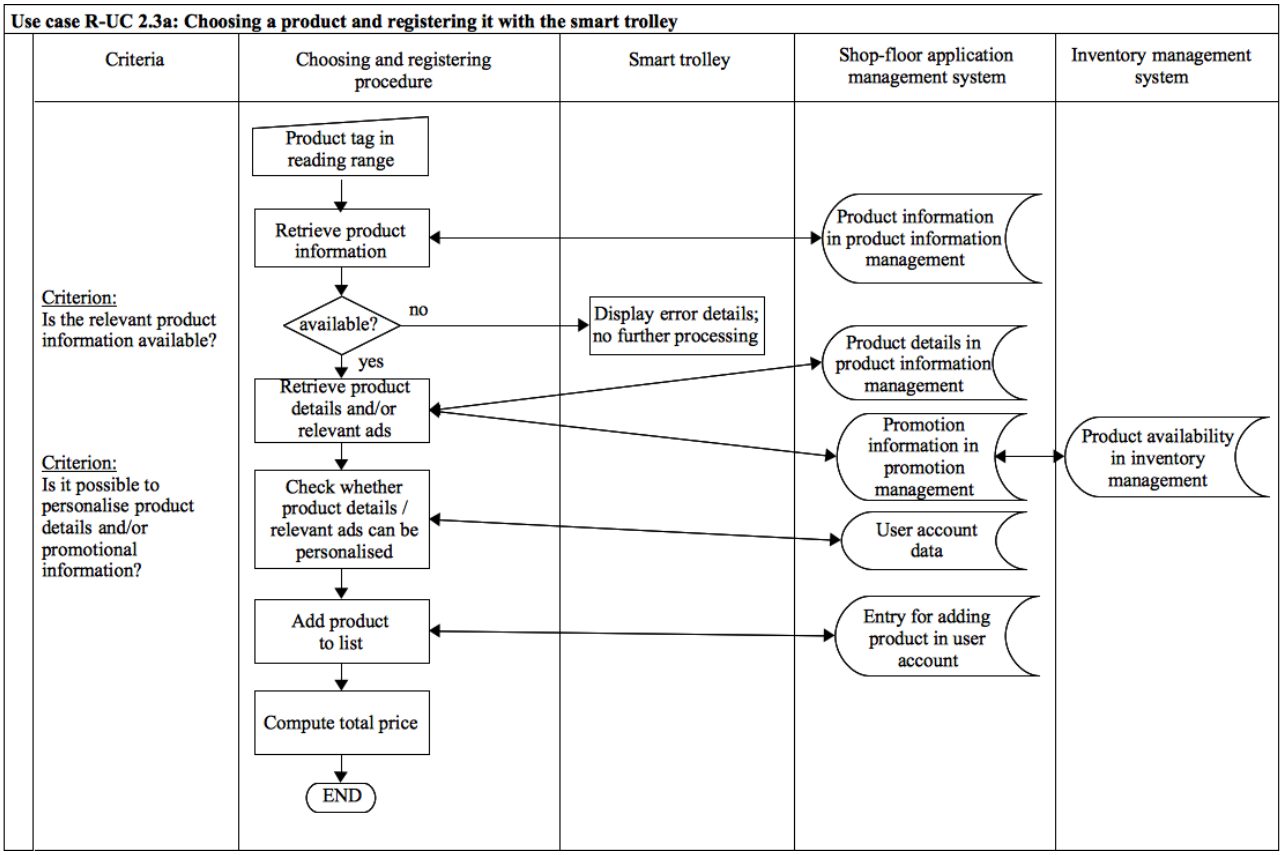

Figure 18: Use case R-UC 2.3a – Choosing a product and registering it with the smart trolley

2.2.1.3.8 Use case R-UC 2.3b: Anonymously choosing a product and registering it with the smart trolley

The use case described in R-UC 2.3a can also be performed by a consumer who has not authenticated with a loyalty card to the smart trolley and is thus shopping anonymously. This results in some differences in the procedure that are described in the following.

Similarly, the tag is read and if there is some product information available in the shop-floor application management system, detailed product information is retrieved and displayed. If no such information is available, an error message is displayed and the registering procedure is aborted.

Additionally, it is checked if some relevant promotion information is available. If this is the case and the corresponding product(s) is (are) available in the store according to the inventory management system, the respective ad(s) is displayed on the trolley's screen, too. Here, no further personalisation is applicable.

The product is then added to the purchase list and the total price of the products that have been put in the trolley is computed and displayed. Here, an entry for adding the product to the purchase list is written into an anonymous user account.

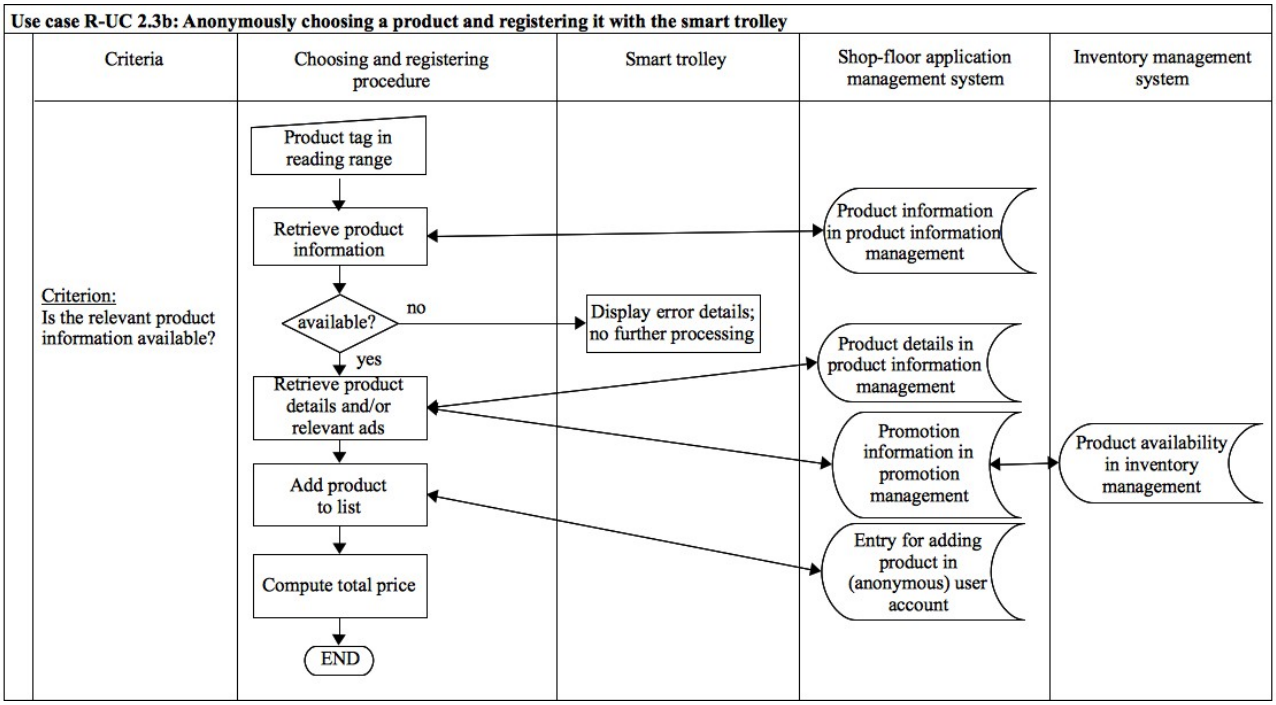

Figure 19: Use case R-UC 2.3b – Anonymously choosing a product and registering it with the smart trolley

2.2.1.3.9 Use case R-UC 2.4a: Walking through the retail store

As already described earlier, throughout the store several readers are positioned in such a way that they can register passing trolleys. That means, that during the consumer's walk through the store, his trolley will be registered by these static readers.

If the trolley's tag comes into the reading range of one of the static readers, a position entry is written to the user account. This entry contains the position ID of the respective static reader, the trolley ID, the user ID and a timestamp.

It is then checked, whether the current position ID equals the position ID of the static reader that is located at the exit of the store. If this is not the case, the movement registration procedure is finished. If it is the case, all position entries, which have been written into the user account during the current shopping visit, are retrieved and a movement profile is created. This movement profile is then written to the user account.

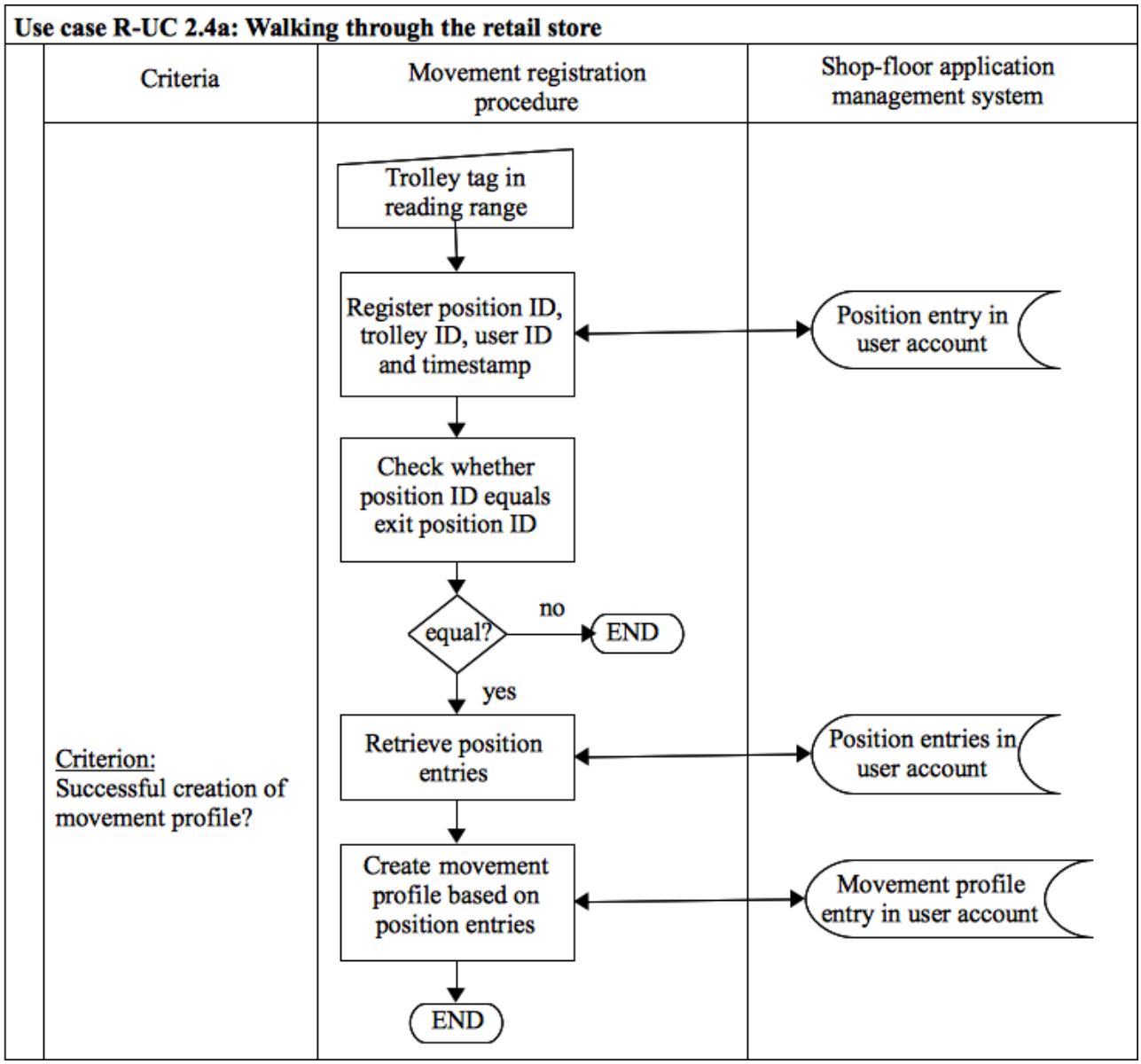

Figure 20: Use case R-UC 2.4a – Walking through the retail store

2.2.1.3.10 Use case R-UC 2.4b: Anonymously walking through the retail store

The use case described in R-UC 2.4a can also be performed by a consumer who has not authenticated with a loyalty card to the smart trolley and is thus shopping anonymously. This results in some differences in the procedure that are described in the following.

If the trolley's tag comes into the reading range of one of the static readers, a position entry is written to an anonymous user account. This entry contains the position ID of the respective static reader, the trolley ID and a timestamp.

It is then checked, whether the current position ID equals the position ID of the static reader that is located at the exit of the store. If this is not the case, the movement registration procedure is finished. If it is the case, all position entries, which have been written into the anonymous user

account during the current shopping visit, are retrieved and a movement profile is created. This movement profile is then written to the anonymous user account.

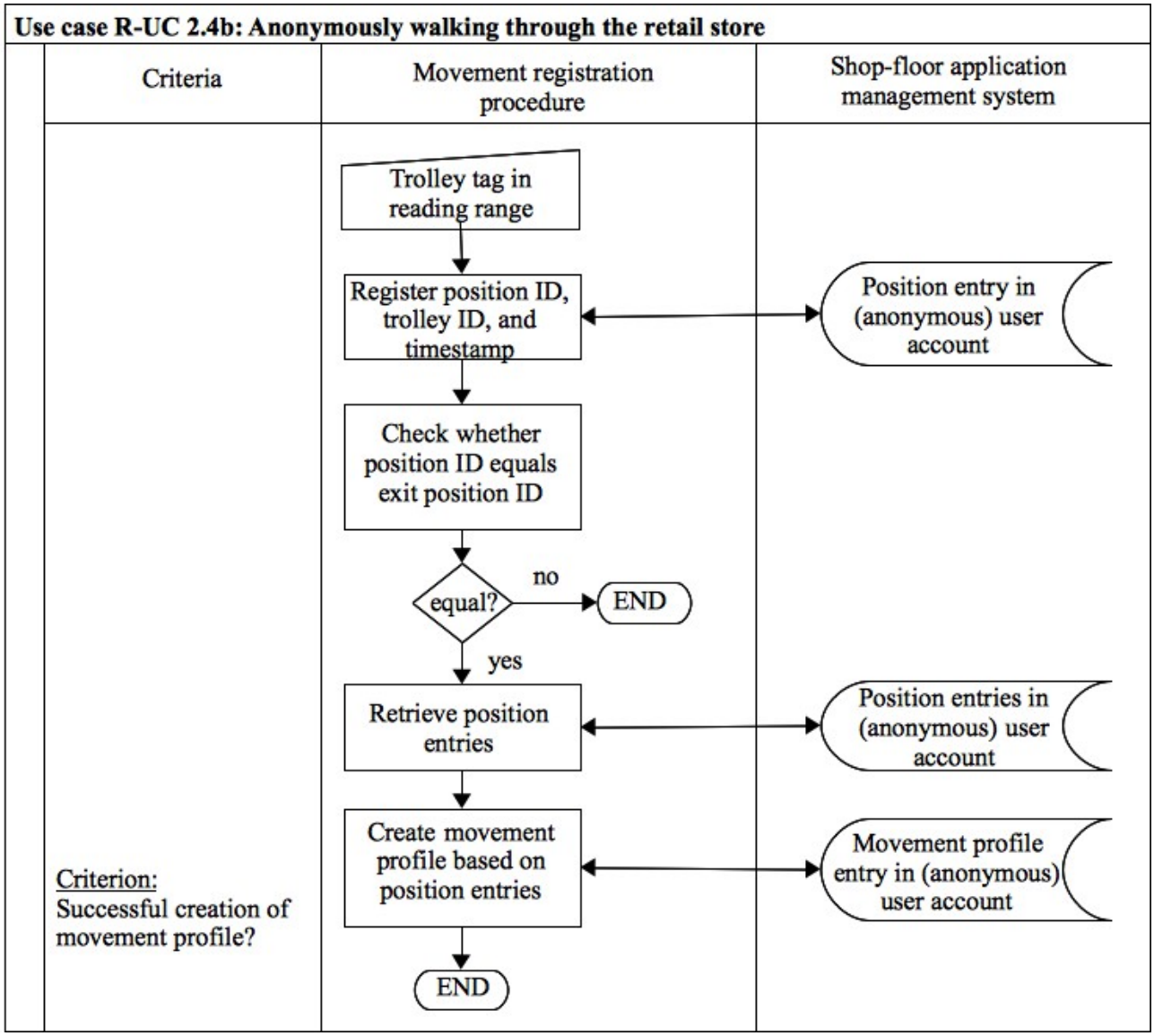

Figure 21: Use case R-UC 2.4b – Anonymously walking through the retail store

2.2.1.3.11 Use case R-UC 3.1: Anonymously taking a product from the shelf and getting information on the screen

This use case is performed anonymously by every consumer as the smart shelf does not ask for a consumer loyalty card.

When the consumer takes a product from the shelf, this is registered by one of the readers that are attached to the smart shelf. But it is not known to the system whether the product has been taken out or put back. This is checked by comparing the inventory of the smart shelf before and after the registered movement. If it is concluded that the product has been put back on the shelf the procedure continues with R-UC 3.2. In the case, that it is concluded, that the product has been taken

out of the shelf, it is checked whether some product information is available. If no product information is available, a back-up ad could be displayed and the procedure is aborted. If product information is available, detailed product information and promotion information is retrieved and displayed. Ads that are derived from the promotion information are only then displayed when the corresponding product(s) is (are) available in the store according to the inventory management system.

Finally, a display entry is written to the shelf's data base that contains the product ID, the ad ID and a timestamp.

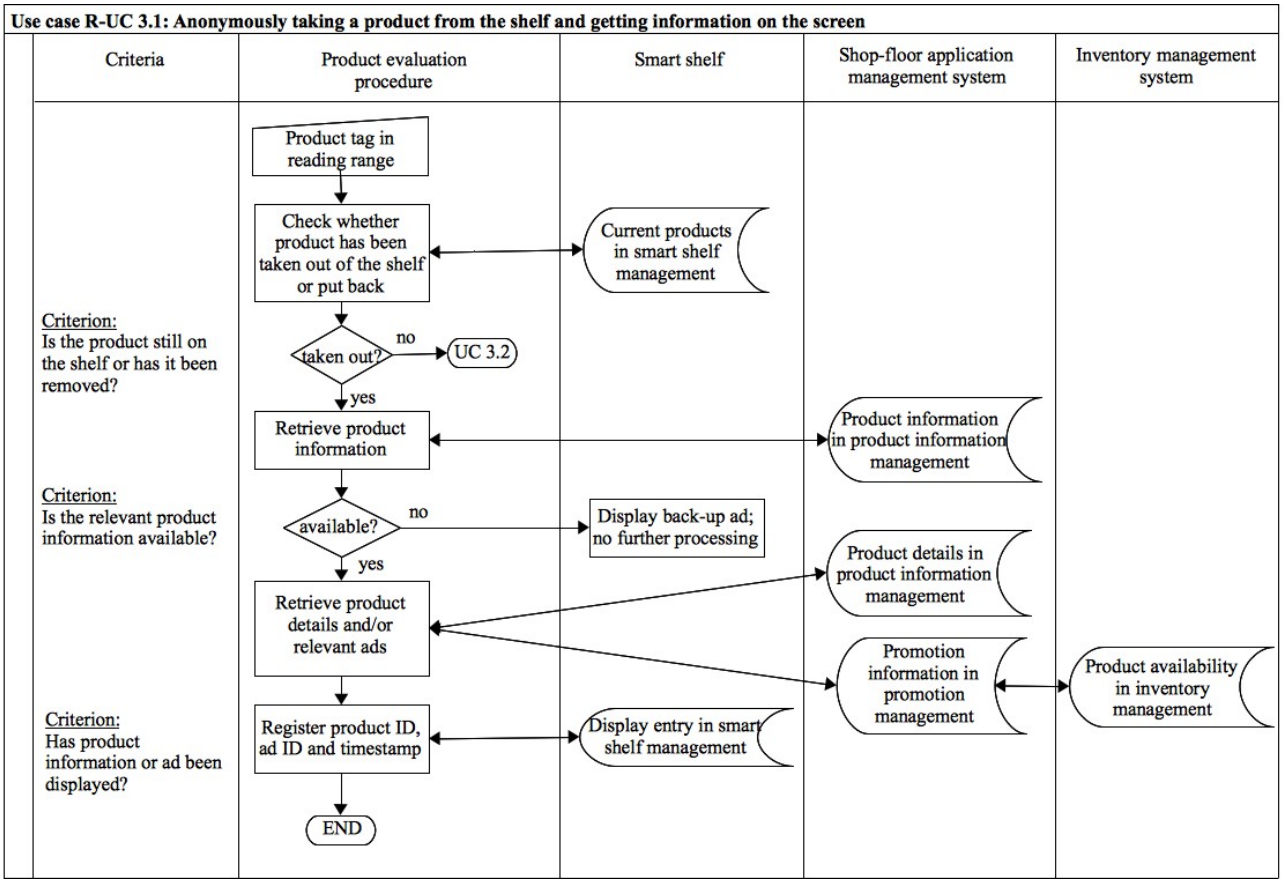

Figure 22: Use case R-UC 3.1 – Anonymously taking a product from the shelf and getting information on the screen

2.2.1.3.12 Use case R-UC 3.2: Anonymously putting a product back on the shelf

This use case is performed anonymously by every consumer as the smart shelf does not ask for a consumer loyalty card.

When the consumer puts a product back on the shelf, this is registered by one of the readers that are attached to the smart shelf. But it is not known to the system whether the product has been taken out or put back. This is checked by comparing the inventory of the smart shelf before and after the registered movement. If it is concluded that the product has been taken out of the shelf the procedure continues with R-UC 3.1. In the case, that it is concluded, that the product has been put back on the shelf, it is checked whether product details or relevant ad(s) have been displayed before. If there is no respective display entry in the shelf's data base, the procedure is finished. If a matching display entry can be found in the shelf's data base, the displaying of the product details or

the ad(s) is considered unsuccessful and an unsuccessful display entry is written to the shelf's data base. These unsuccessful display entries are - at a later point in time - aggregated and forwarded to the shop-floor application management system, which can then perform an analysis comprising data from all smart shelves of the store.

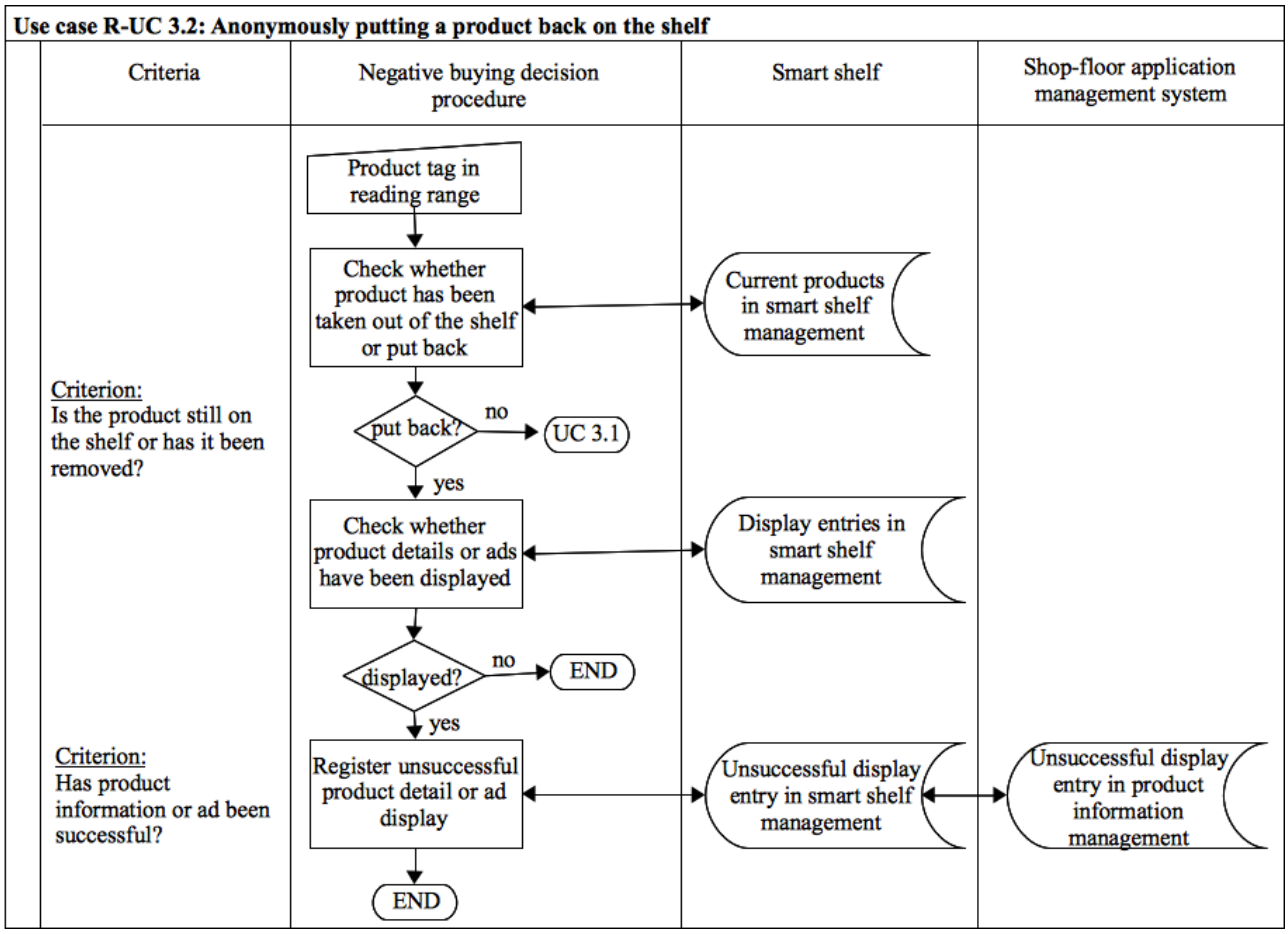

Figure 23: Use case R-UC 3.2 – Anonymously putting a product back on the shelf

2.2.1.3.13 Use case R-UC 4.1: Putting products on the conveyor belt

As described earlier, the self-checkout offers the consumer the possibility to choose wether the tags of the products he is purchasing shall be killed, put asleep or remain active. The consumer can define the desired outcome for each of the products and then groups them on the conveyor belt accordingly. The products are then processed one after another following the below-described procedure.

A product tag is read, the respective product information is retrieved and it is checked whether the consumer defined to kill, put asleep or leave active the product's tag. In the case, the consumer chose to leave the product's tag active, the procedure continues in the next paragraph. If the consumer chose to kill or put asleep the product's tag, the respective kill or put asleep password is retrieved from the tag management system and is executed. The successful killing or putting-asleep of the tag is displayed to the consumer.

The product is then added to the purchase list and the purchase list entry in the self-checkout's data base is updated accordingly. Finally, the total price is computed and the respective entry in the self-checkout's data base is updated, too.

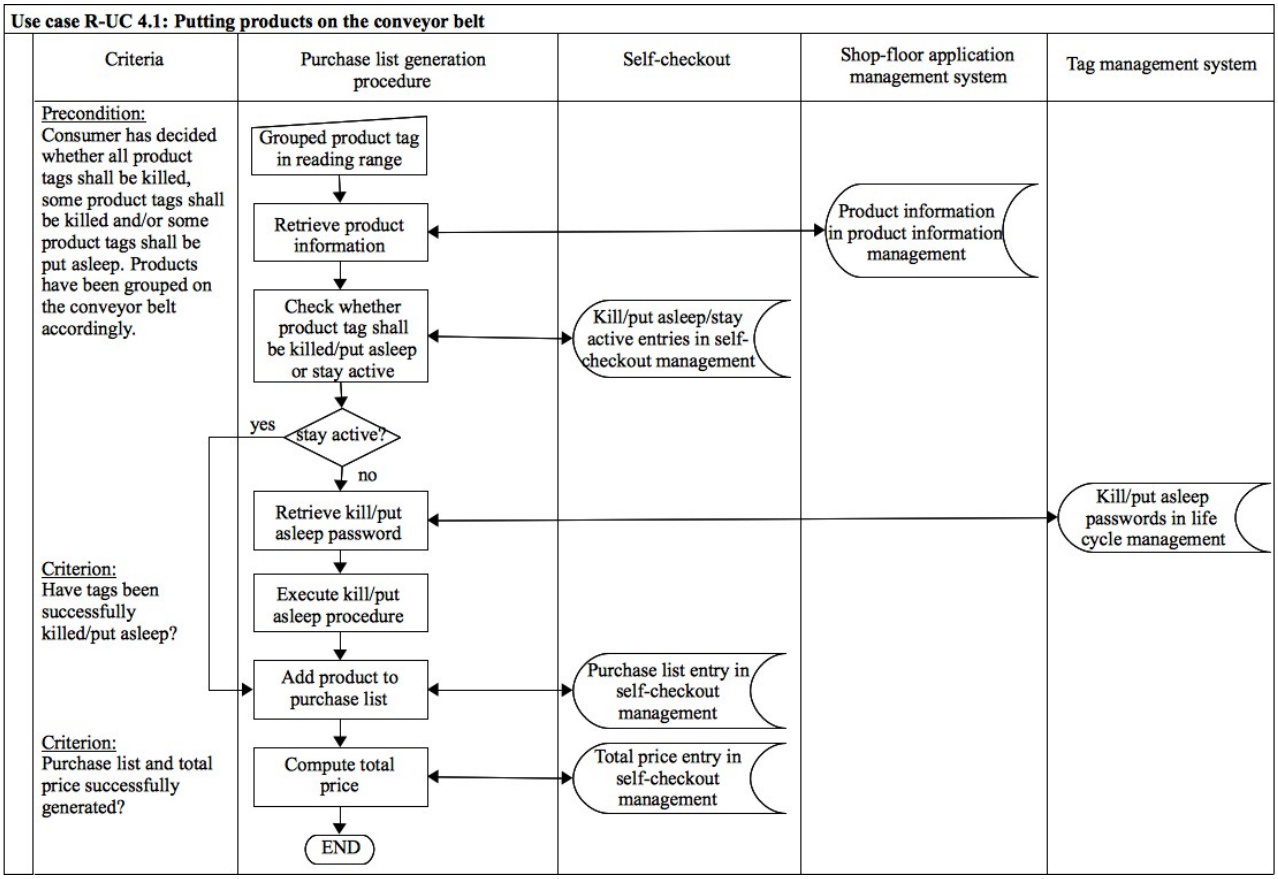

Figure 24: Use case R-UC 4.1 – Putting products on the conveyor belt

2.2.1.3.14 Use case R-UC 4.2a: Purchasing the products

To finalize the purchase and before providing the payment, the consumer holds his loyalty card to the self-checkout's reader.

It is checked whether any coupons or discounts are available. These can either be

- personalised
  In this case, the user account data is checked for personalised discounts and/or coupons.
- or of general nature
  In this case, the general promotional information of the promotion management is checked for current discounts and/or coupons that are available for every consumer.

If there are any, the total price is decreased accordingly and a discount entry is written to the user account to signal that the discount/coupon has been cashed. The total price entry in the self-checkout's data base is updated with the decreased price. Then the payment transaction is completed by either providing cash, credit card or the like. The respective payment type is registered in the user account of the consumer.

Finally, the outgoing products are registered in the self-checkout's data base and are forwarded to the inventory management system.

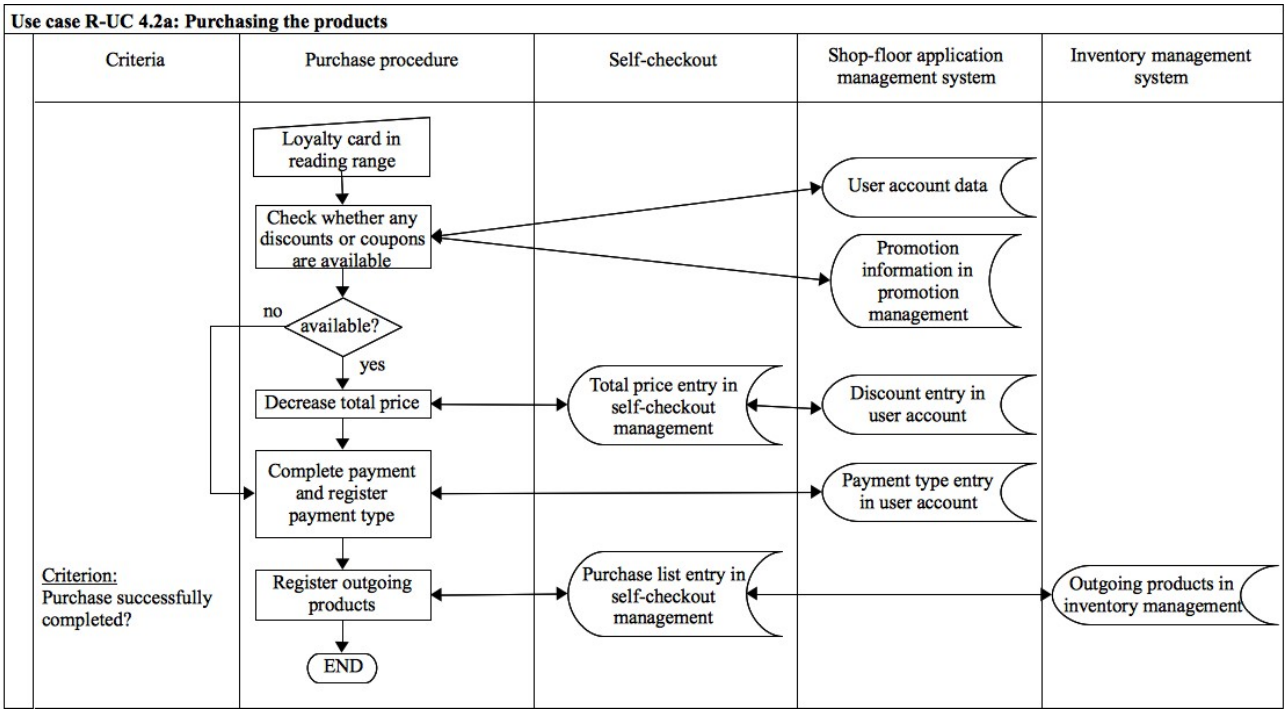

Figure 25: Use case R-UC 4.2a – Purchasing the products

2.2.1.3.15 Use case R-UC 4.2b: Anonymously purchasing the products

The use case described in R-UC 4.2a can also be performed by a consumer who has not provided a loyalty card to the self-checkout and is thus shopping anonymously. This results in some differences in the procedure that are described in the following.

It is checked whether any coupons or discounts are available. These can only be of general nature, thus, the general promotional information of the promotion management is checked for current discounts and/or coupons that are available for every consumer. If there are any, the total price is decreased accordingly and a discount entry is written to an anonymous user account to signal that the discount/coupon has been cashed.

The total price entry in the self-checkout's data base is updated with the decreased price. Then the payment transaction is completed by either providing cash, credit card or the like. The respective payment type is registered in the anonymous user account.

Finally, the outgoing products are registered in the self-checkout's data base and are forwarded to the inventory management system.

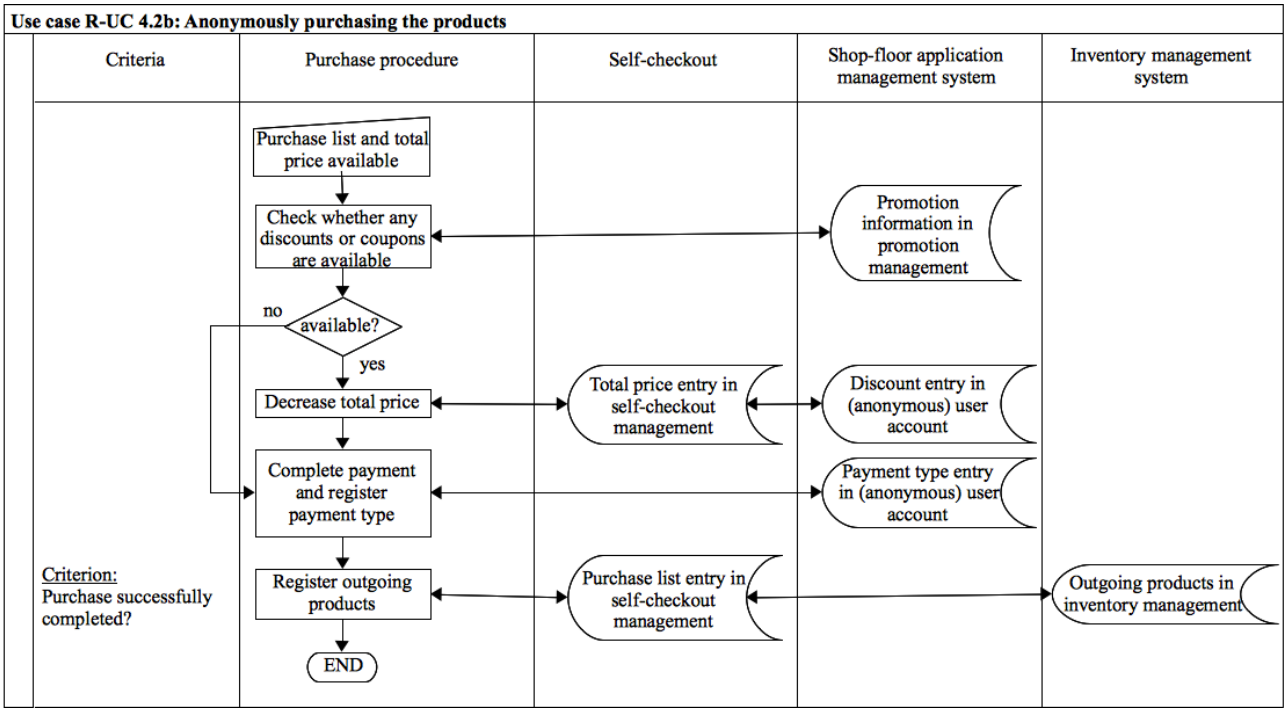

Figure 26: Use case R-UC 4.2b – Anonymously purchasing the products

2.2.1.3.16 Use case R-UC 4.3: Leaving the retail store

When the consumer leaves the store, he passes some readers that have been positioned at the exit of the store. All product tags of his purchase that are still readable, are read by these readers. Product tags that have been killed during checkout cannot be read.

The corresponding product information is retrieved and it is checked whether the product can be identified as one of the outgoing products. This check is realised with the help of the outgoing product entries in the inventory management. If the product actually is one of the outgoing ones, the procedure is finished. If it cannot be identified to be outgoing, an alarm is triggered.

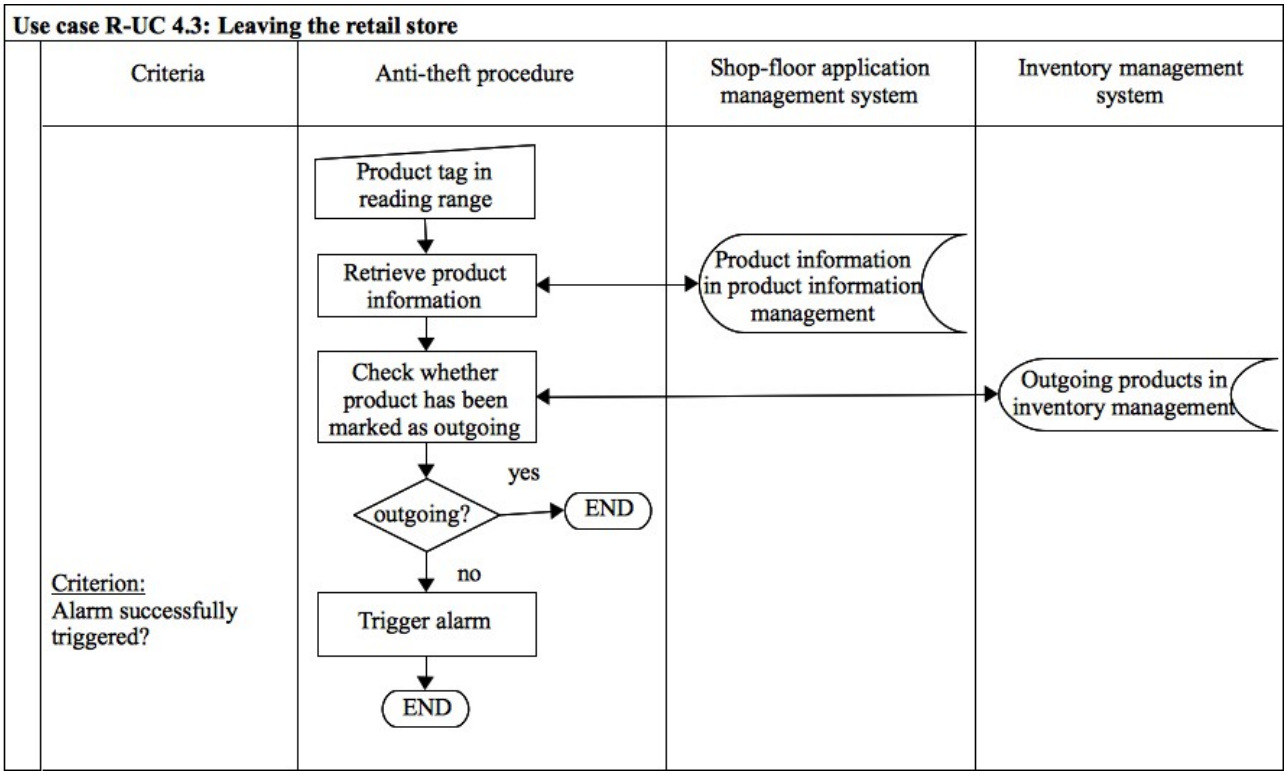

Figure 27: Use case R-UC 4.3 – Leaving the retail store

2.2.1.3.17 Use case R-UC 5.1: Registering for the added-value service

The consumer needs to fill out a registration form to register for the added-value service. This can most probably be done via a web application. The application ensures that all necessary personal data has been provided by the consumer. In the simplest case, the consumer might only provide an email address. This can either be

- an email address containing his name
  In this case, the consumer decides to register in a personalised way. He most likely will also provide additional personal information that might be relevant for the service. Furthermore, if necessary, he can prove his identity by providing his eID to the application.
- an email address containing a pseudonym
  In this case, the consumer decides to remain anonymous in the realm of the added-value service. It is only possible to link to his personal data via the respective email account.
- or an anonymous email address
  In this case, the consumer decides to remain anonymous in the realm of the added-value service.

The registration form is then processed and a user account containing the consumer's personal data is created in the added-value service management system.

Finally, the consumer can register the product, e.g. the running shoe, he wants to use in conjunction with the added-value service with the system. A product entry is then written to the user account.

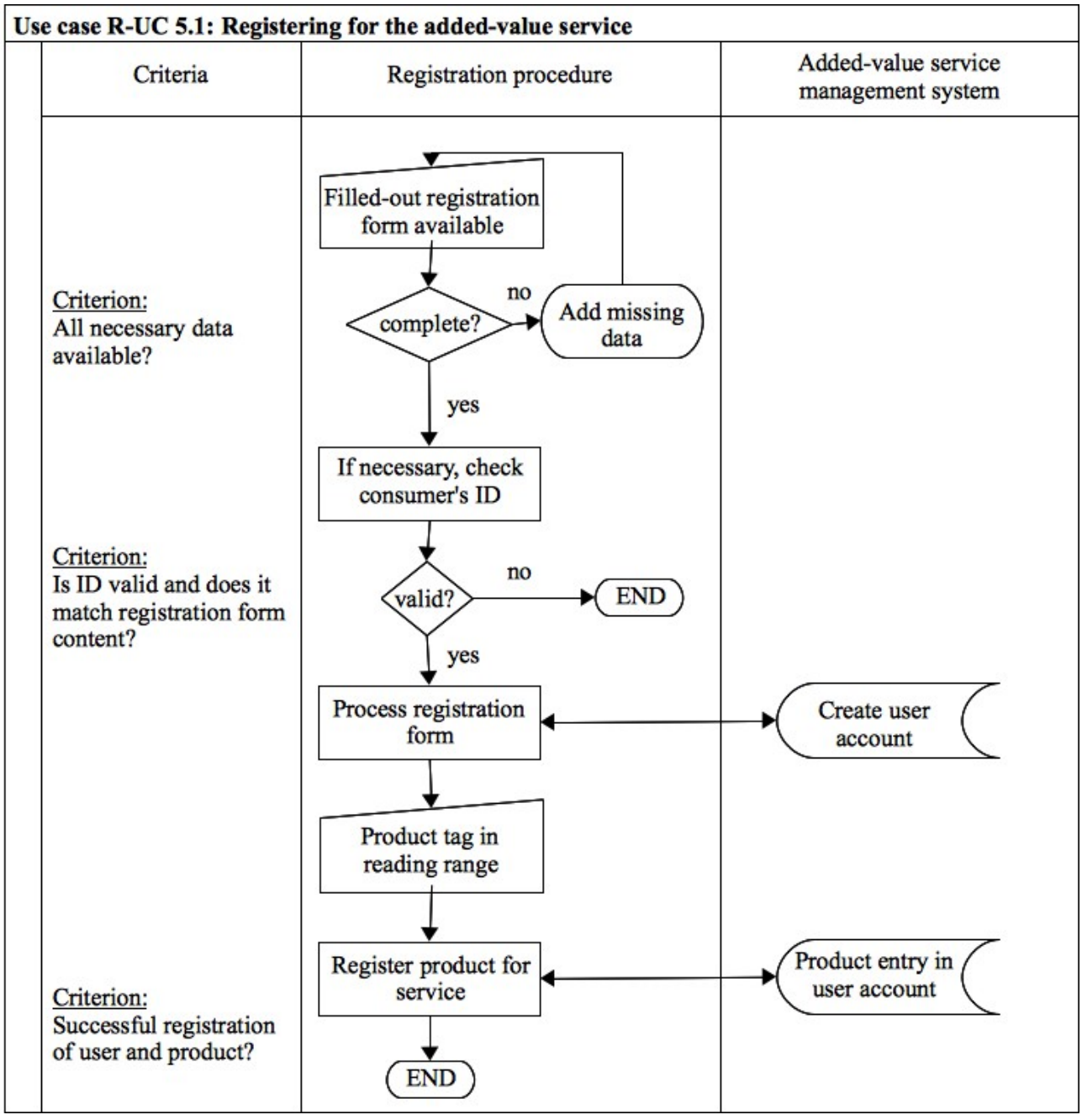

Figure 28: Use case R-UC 5.1 – Registering for the added-value service

2.2.1.3.18 Use case R-UC 5.2: Using the added-value service

Coming back to the example described earlier, the consumer uses a running shoe which contains a tag and separately provides a reader that can be connected to a handheld device. During usage the tag then continuously transmits data to the handheld device.

When the consumer finished his running exercise, he connects the handheld device to the Internet and accesses the web application of the added-value service using his user account. Then the data is transferred to the application and a respective usage data entry is written to the user account.

The uploaded data is then e.g. visually displayed according to the user's preferences and personalised feedback concerning his exercise is provided, combining existing usage entries in the user account with general feedback information from the service.

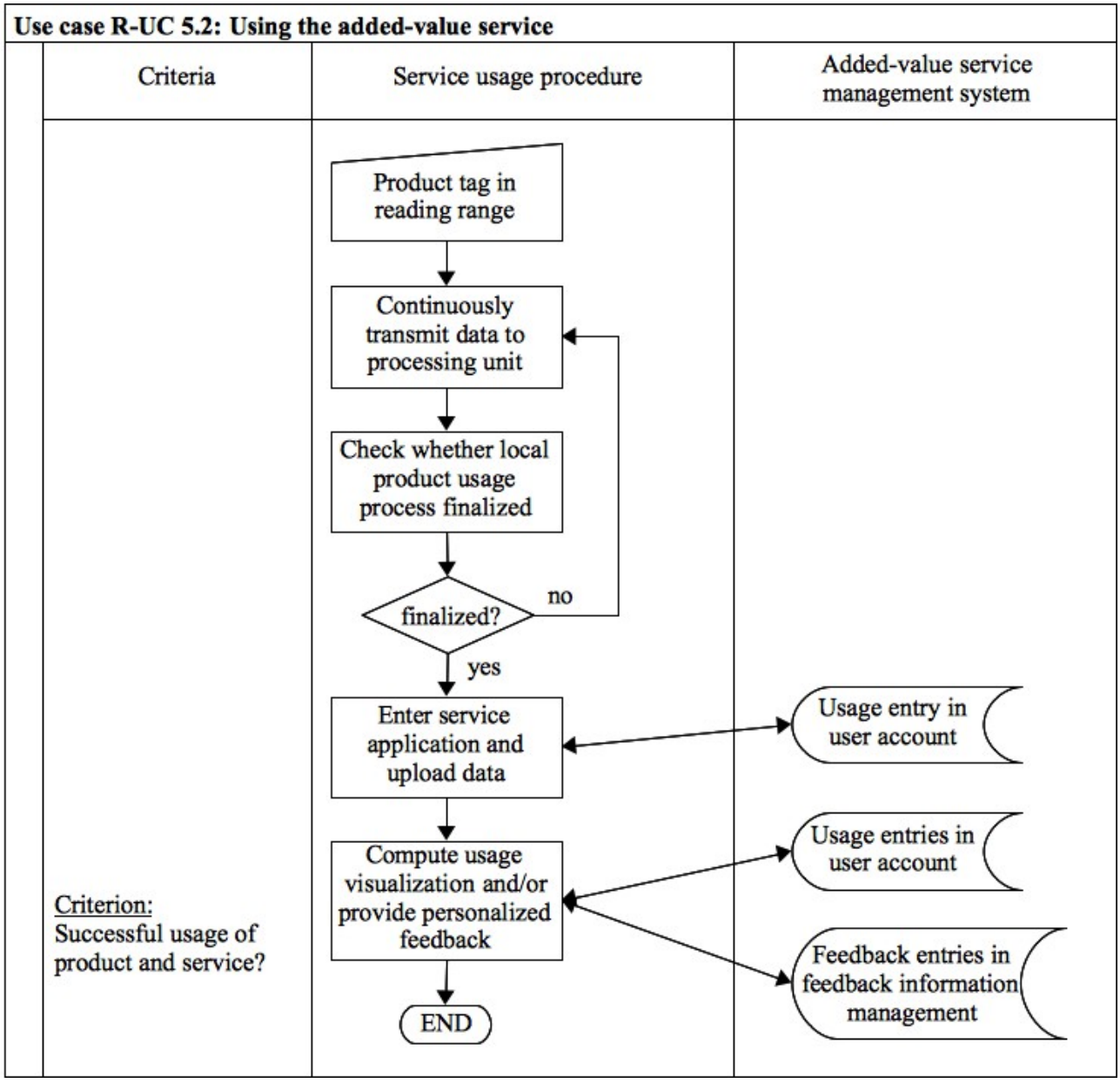

Figure 29: Use case R-UC 5.2 – Using the added-value service

2.2.1.3.19 Use case R-UC 5.3: De-registering from the added-value service

The prerequisite for this use case is the application of a consumer for a de-registration. The de-registration request is only accepted and filed for further processing after positively identifying the consumer.

When a de-registration request has been filed, the respective data is retrieved from the user account. The user account is then blocked and the account-specific black- and whitelists are updated accordingly. Consequently, the consumer cannot use his user account anymore.

The next step of the de-registration procedure is to add a de-registration entry to the user account. It then needs to be checked whether the user account has to be deleted. If it does not contain any personal data or references to personal data its data could be saved by the added-value service provider and further used for analysis purposes. If the user account contains personal data or the added-value service provider does not want to keep the data, the deletion of the user account is scheduled. Now starts a dedicated period of time during which the consumer can take back his de-registration request. Only when this period of time elapses, the actual deletion of the user account is performed.

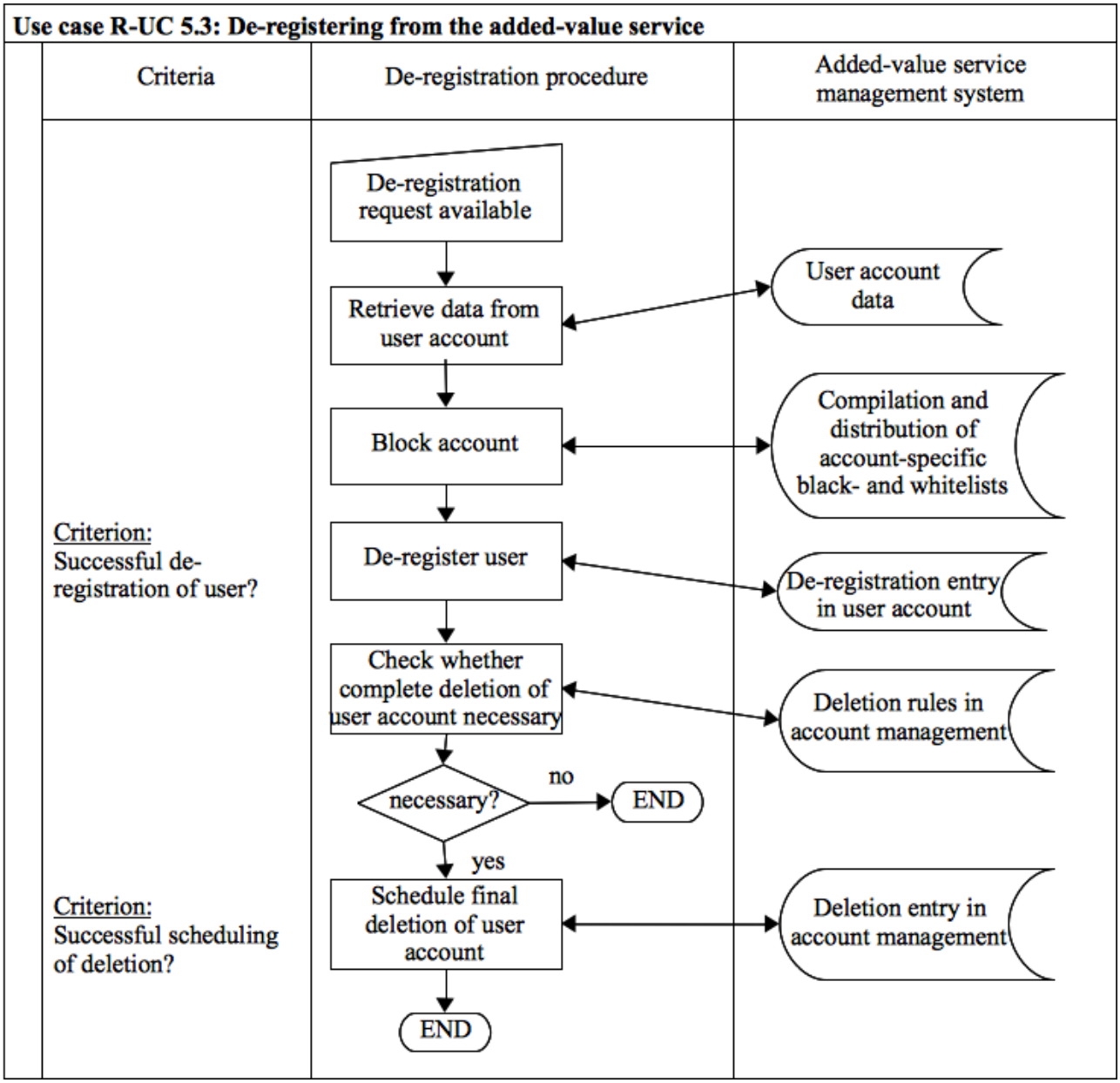

Figure 30: Use case R-UC 5.3 – De-registering from the added-value service

2.2.1.3.20 Use case R-UC 6.1: Depersonalising the tag

A depersonalisation procedure is offered by the added-value service provider. Thus, the consumer can depersonalise the tag of his product before handing it over to another person or before disposing it. This procedure can either be performed via a web application at home or at a service point where the product, respectively its tag, is put in front of a reader.

First it is checked whether the tag is valid and can actually processed by the depersonalisation procedure. If not, e.g. if it is a product tag that is not related to the added-value service at hand, the procedure aborts. In the other case, it is checked whether any of the tag's IDs is linked to personal data in the user account. If this is not the case, the procedure is finished because the tag does not

need to be depersonalised. If there is a link to some personal data, it is checked whether the linking ID can actually be deleted from the tag, e.g. in the case of a tag's serial number this would not be possible. If the ID is not deletable, the procedure continues in R-UC 6.3. If it is deletable, the deletion is executed.

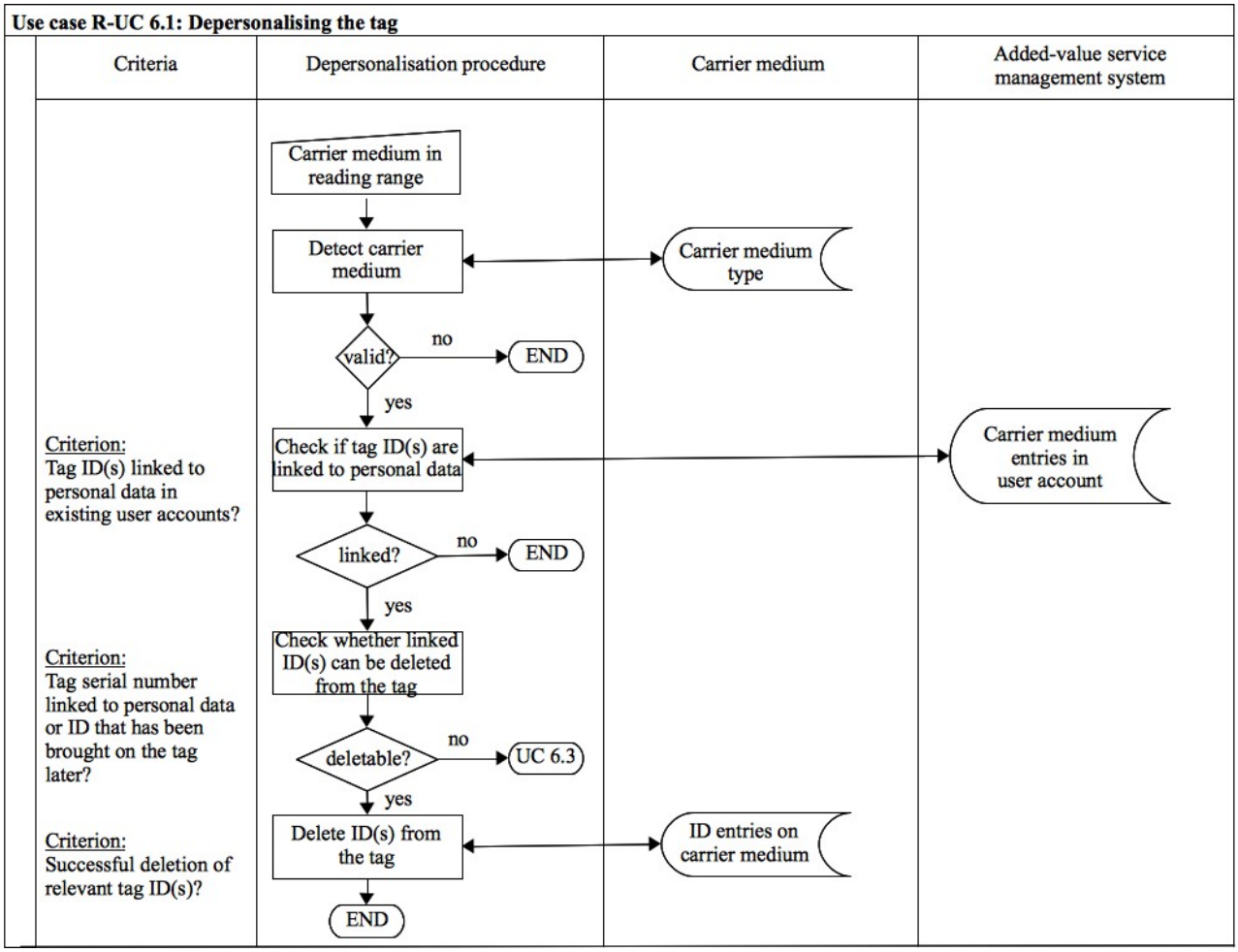

Figure 31: Use case R-UC 6.1 – Depersonalising the tag

2.2.1.3.21 Use case R-UC 6.2: Re-personalising the tag

Re-personalisation can either happen via writing a new ID onto the tag or linking an existing ID to personal data of the new product owner.

2.2.1.3.22 Use case R-UC 6.3: Destroying the tag

The tag can either be destroyed manually or electronically. The destruction procedure might be offered by the added-value service provider as well, or by the retailer/manufacturer. Again, this procedure can either be performed via a web application at home or at a service point where the product, respectively its tag, is put in front of a reader.

First it is checked whether the tag is valid and can actually processed by the destruction procedure. If not the procedure aborts. In the other case, the respective kill password is retrieved from the tag management system and is executed. The successful killing of the tag is displayed to the consumer.

This use case deals with the same topic as "Activating the kill command" from [BSI2008], page 69. Nevertheless, it describes the destruction procedure from a slightly different perspective, namely omitting some of the technical details and focussing on privacy relevant aspects.

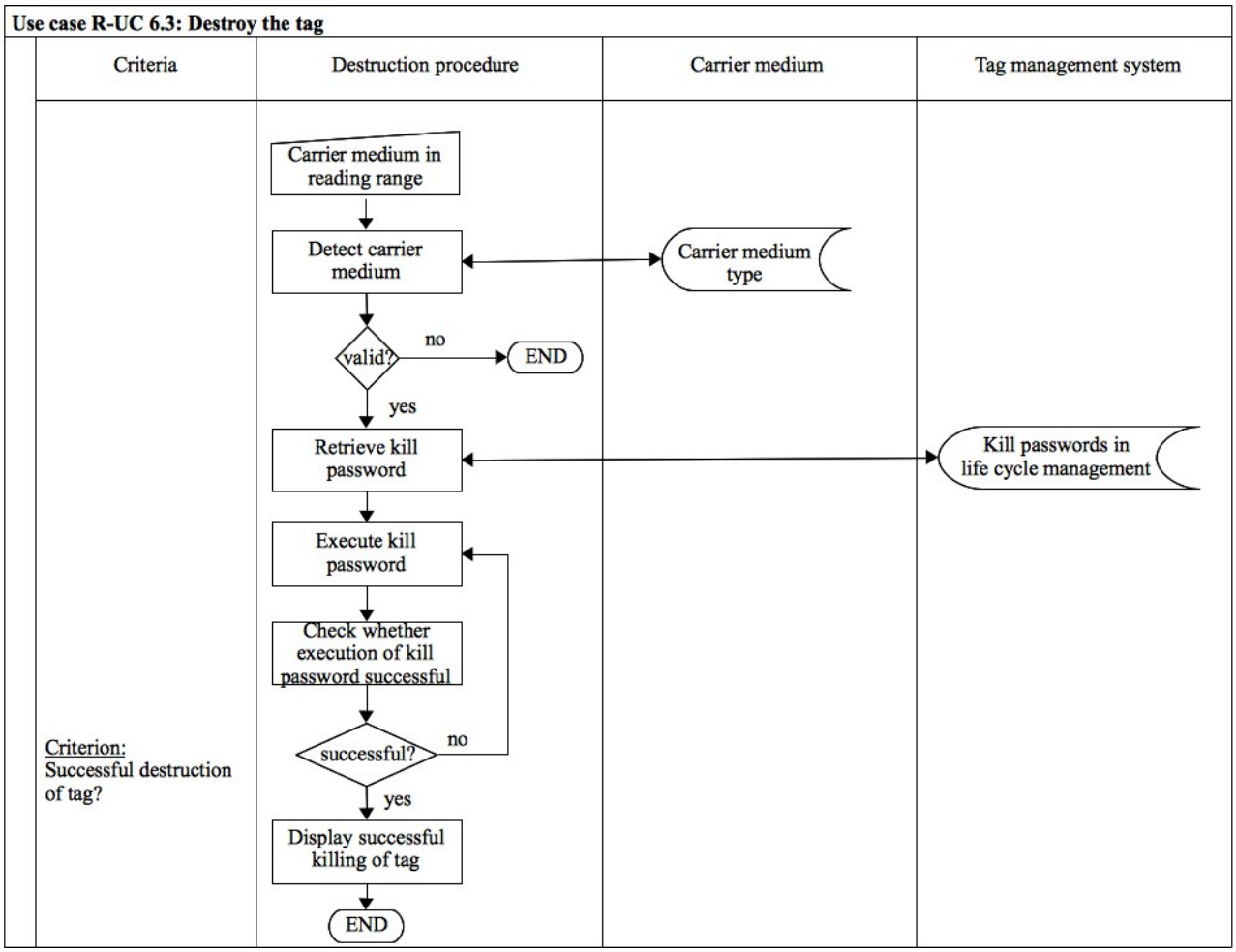

Figure 32: Use case R-UC 6.3 – Destroying the tag

2.2.2 Step 2: Definition of privacy targets

In this step, stakeholders should discuss the privacy targets that are described in the PIA Framework and the concrete instances of those privacy targets as described in the PIA guideline. By discussing the targets and their instances, stakeholders can clarify what the targets mean in the context of the specific RFID application and corresponding business cases.

Privacy target code and name		**Contextual explanation**	**Examples for how to reach this target**
P1.1	Ensuring fair and	The operator must create internal and external	Use the RFID-emblem, flyers, web

Privacy target code and name		Contextual explanation	Examples for how to reach this target
	lawful processing through transparency	transparency by explaining the RFID technology used and the data flows involved in operating the loyalty card, the shop-floor applications and the added-value service. This information should be easily understandable and accessible for every consumer. Consumers and employees should be able to understand the benefits and consequences of participating in the loyalty program and/or using shop-floor applications.	pages, documentation and/or training for employees who have consumer contact.
P1.2	Providing purpose specification and limitation	The operator must explicitly specify why consumer data is collected during the loyalty program and how the shop-floor applications and added-value service is used. It should be clear what data is used for which purposes, what data is linked and what data might be given to a third party.	Document whether consumer data for the loyalty program is linked to usage data of the shop-floor applications. Document whether consumer data is handed over to added-value service providers.
P1.3	Ensuring data avoidance and minimisation	The operator must aim to design and implement the loyalty program, the shop-floor applications and the added-value service so that only necessary consumer data is collected and processed. In this context, necessary means that the data is required for the fulfilment of the specified purpose.	Offer the consumer a choice between personalised, pseudonymous and anonymous usage of the services (R-P1).
P1.4	Ensuring quality of data	The operator must ensure that consumer data is correct and up-to-date. This data is stored in the user account management system of the shop-floor application, the added-value service management system and consumer account of the CRM system.	Check the registration forms (R-P1.1, R-P5.1) thoroughly. Regularly remind the consumers to check that their user accounts are correct and up-to-date.
P1.5	Ensuring limited duration of data storage	For all the applications used in the scenario, consumer data must be stored only as long as legally required or necessary for the specified purpose.	Institute strict erasure rules that are executed when a consumer de-registers (R-P1, R-P5).
P2.1	Legitimacy of processing personal data	When a consumer participates in the loyalty program, check the validity of his or her consent.	Check the registration forms (R-P1.1, R-P5.1) thoroughly.
P3.1	Legitimacy of processing sensitive personal data	- not applicable in this scenario - No sensitive personal data is collected or processed in this scenario.	- not applicable in this scenario -
P4.1	Providing adequate information in cases of direct collection of data from the data subject	Data is directly collected from the consumer through the loyalty card registration form and the workings of the shop-floor applications as well as the added-value service.	Provide adequate information, see P1.1.

Privacy target code and name		Contextual explanation	Examples for how to reach this target
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	- not applicable in this scenario - No data that is directly obtained from the consumer, e.g. data from third parties, is processed in this scenario.	- not applicable in this scenario -
P5.1	Facilitating the provision of information about processed data and purpose	The consumer can access all relevant information on whether and how his or her data is used by the RFID operator. Hence the consumer has a contact point at the RFID operator where it is possible to ask questions about subjects such as the existence of personal data, the purposes 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.	Offer a call-centre, contact address or online interface where consumers can ask for their personal information to be stored, processed and/or transferred.
P5.2	Facilitating the rectification, erasure or blocking of data	The operator must ensure that consumers are allowed to rectify, erase or block their data. The shop-floor application, the added-value service management systems and the CRM system must all be considered.	Offer a call-centre, contact address or online interface where consumers can rectify, erase or block data about themselves via a web application.
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	- not applicable in this scenario - No consumer data is handed over to a third party in this scenario.	- not applicable in this scenario -
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	The operator must ensure that consumers are allowed to object to the processing of their data for direct marketing purposes or disclosure to third parties. There is no disclosure of consumer data to third parties in this scenario. Consumer data is used for the purpose of direct marketing as part of the loyalty program.	Offer a call-centre, contact address or online interface where consumers can object to the processing of their data for direct marketing purposes. If consumers object, they may not be able to participate in the loyalty program, as direct marketing is a crucial aspect of this program.
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	The operator must ensure that consumers are allowed to object to being subject to automated decisions. In the loyalty program, discounts and coupons (R-P4) are assigned to each consumer based on automated decisions. Personalisation that happens throughout the shop-floor applications (i.e. smart trolley display) is based on automated decisions too.	Offer a call-centre, contact address or online interface where consumers can object to such automated decisions. This may implicate that they cannot participate in the loyalty program and added-value service as personalisation is a crucial aspect of these services.

Privacy target code and name		Contextual explanation	Examples for how to reach this target
		Added-value services (R-P5.2) are also subject to automated decisions.	
P7.1	Safeguarding confidentiality and security of processing	BSI's TG 03126-4 needs to be considered.	---
P8.1	Compliance with notification requirements	Before going live with the shop-floor applications, the loyalty program and the added-value service, the supervisory data protection authority needs to be notified about the related processing of personal data. There is the need to provide the results of the PIA to the supervisory authority six weeks before the launch.	The retailer and the added-value service provider should assign a person in their organisation to take care of these notifications. The assignee might need a project team to create the necessary documentation.

Table 8: Retail PIA – Definition of privacy targets

2.2.3 Step 3: Evaluation of protection demand categories

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.1	Ensuring fair and lawful processing through transparency	2	2	1	1	2	2

If the data processing activities related to the system landscape are not made transparent internally as well as externally to consumers or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if consumers are misinformed (i.e. by call-centre employees, shop employees) or if consumers misjudge the degree of personal data processing involved in the services. A lack of transparency can also lead to limited or contradictory information being picked up by journalists. Finding out about more data processing and use taking place than expected can lead consumers to feel betrayed. In particular, negative press resulting from a lack of transparency is a danger for a company's reputation.
- the operator's financial loss can be considerable when a lack of transparency leads to negative press, consumer backlash, or both. Consumers may avoid visiting retail stores. Image campaigns may be necessary to restore consumers' faith. Stock market valuation can suffer (at least in the short term) when unlawful processing becomes known to the public.
- consumers' reputation can be adversely affected if, without their prior knowledge, information about their purchases and service-use are used for judgements about them (i.e. concerning their creditworthiness, etc.).
- consumers' financial well-being can be adversely affected if, without their prior knowledge, information about their purchases and service-use is used so segment them into groups that disallow access to financially

advantageous offerings (i.e. coupons or discounts only accessible to consumers with certain traits).

- consumers' personal freedom could be endangered because they decide to participate in a service, but base this decision on limited information about the data processing activities involved.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 9: Retail PIA – Definition of protection demand categories for P1.1

Privacy target code and name		**Criteria for the classification of protection demand categories**					**Overall category**
		Operator perspective		**Consumer perspective**			
		Impact on Reputation and Brand Value	**Financial loss**	**Social standing, reputation**	**Financial well-being**	**Personal freedom**	
P1.2	Providing purpose specification and limitation	2	2	2	2	1	2

If the purpose and limitations of data processing are not specified, the RFID operator risks engaging in processing that is beyond the purposes for which data has been initially collected from data subjects. If such processing becomes known to the public, consumers, journalists or the authorities, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if detailed data about consumers' shopping behaviour is used for purposes that were not specified and are accessed by unauthorised parties. Consumers can feel betrayed. Journalists can accuse the company of lying to their consumers and abusing personal data.
- the operator's financial loss can be considerable when the damage to its reputation causes consumers to stop visiting retail outlets, and costly image campaigns are needed to restore the consumers' faith. Legal trials may ensue. Sanctions may be imposed by the authorities.
- consumers' reputation can be seriously adversely affected if their individual shopping behaviour (i.e. shopping paths and time, interests for intimate product categories, unusual purchase patterns for sensitive items, etc.) becomes known to unauthorised parties and may be used for purposes that were not specified and agreed upon.
- consumers' financial well-being can be seriously adversely affected if their individual shopping behaviour becomes known to unauthorised parties (i.e. employers, insurance companies, creditors, etc.) and may be used for purposes that were not specified and agreed upon.
- consumers' personal freedom cannot be endangered.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 10: Retail PIA – Definition of protection demand categories for P1.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.3	Ensuring data avoidance and minimisation	2	2	2	2	1	2

The retailer wants to minimise consumers' privacy concerns as well as information and notification duties that depend on the amount of personal data processed. More data also implies a need for the often costly implementation of sophisticated technical controls to secure the collected personal data.

If the principles of data avoidance and minimisation are not realised throughout the relevant applications and services, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if consumers who are considering registration for a loyalty card or after-sales service perceive that too much data is being requested from them in the sign-up process. Due to privacy concerns, some consumers may decide not to register at all or are left with an uneasy feeling about the volume of personal data being requested from them.
- the operator's financial loss can be considerable if he invests in a large scale CRM system, but many consumers decide not to participate in the loyalty scheme or value-add services for privacy reasons. Financial implications could also result from an unmanageable data volume.
- consumers' reputation can be seriously adversely affected if personal information that goes beyond their shopping behaviour becomes known (i.e. due to unmanageable data volumes becoming an attractive target for internal and external fraudulent activities).
- consumers' financial well-being can be seriously adversely affected if large data volumes allow for detailed insights into consumers' social status and willingness to pay, which again may be used for price differentiation.
- consumers' personal freedom cannot be endangered because the amount of data collected in this scenario does not increase its potential to limit their freedom.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 11: Retail PIA – Definition of protection demand categories for P1.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.4	Ensuring quality of data	2	2	1	1	1	2

The retailer wants to deliver services that result in satisfied consumers and make recommendations that are useful. If these goals are met, the number of purchases will increase and people will be drawn to the stores because of recommendations that were made for them (i.e. through personalized mailings, coupons, etc.). As the quality of the services strongly depends on the accuracy of the original and aggregated data, the operator should invest in measures that ensure the quality of the collected consumer data.

If the quality (accuracy, up-to-dateness or completeness) of the personal data that is collected and processed is not ensured, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired when consumers receive mailings or service recommendations that contain spelling mistakes in their names, poorly targeted recommendations, or even offerings that are not foreseen for them. Equally, consumers may be treated by the operator (i.e. by an operator's call-centre or retail staff) in a manner that isn't in line with their loyalty track record.
- the operator's financial loss can be considerable if consumers do not see any value in the recommendations they receive or are even put off (by false judgements). In this case, the operator has invested in a CRM system that doesn't lead to the expected returns. Equally, consumers could decide to drop out and avoid the company in the future.
- consumers' reputation can be adversely affected if they are treated (i.e. by an operator's call-centre or retail staff) in a manner that isn't in line with their loyalty track record.
- consumers' financial well-being can be adversely affected if they do not the receive the discounts or advantages that are appropriate for their category.
- consumers' personal freedom cannot be endangered because even if some of their data was incorrect, the kind of data processed in this scenario would not be life threatening to the individual or limit her freedom.

As two of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 12: Retail PIA – Definition of protection demand categories for P1.4

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.5	Ensuring limited duration of data storage	1	2	2	2	1	2

The retailer wants his consumers to trust him; to some extent it may be argued that *excessive* storage of personal data about consumers is not in line with the belief in a mutually trusting relationship. In addition, management and storage of huge amounts of data are costly.

If data is stored longer than necessary and no clear rules are implemented to limit data storage, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired.
- the operator's financial loss can be considerable if financial implications result from an unmanageable data volume.
- consumers' reputation can be seriously adversely affected if personal information is stored for so long that an unmanageable data volume is created and becomes an attractive target for internal and external fraudulent activities.
- consumers' financial well-being can be seriously adversely affected if large data volumes allow for detailed insights into consumers' social status and willingness to pay, which again may be used for price differentiation.
- consumers' personal freedom cannot be endangered because even if some of their data was stored longer, the kind of data processed in this scenario would not be life threatening to the individual or limit her freedom.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 13: Retail PIA – Definition of protection demand categories for P1.5

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P2.1	Legitimacy of processing personal data	3	2	2	2	2	3

The retailer wants his consumers to trust him and does not want to come into conflict with the law.

If the legitimacy of processing personal data is not ensured, e.g. via consent, the parties that are involved may face the following consequences:

- the operator's reputation can suffer a nation-wide impairment if consumers feel heavily betrayed and might initiate lawsuits.
- the operator's financial loss can be considerable if the reputation's nation-wide impairment leads to costly image campaigns, the cancelling of the planned RFID-enabled applications and services and costs for potential lawsuits.
- consumers' reputation can be seriously adversely affected if personal data is collected, stored and processed in a way that they were not aware of; these processes could lead to false and embarrassing judgements about them.
- consumers' financial well-being can be seriously adversely affected if personal data is collected, stored and used in a way that they were not aware of, leading to false judgements about character, creditworthiness, or other personality traits that can lead them to be disadvantaged in future contracts.
- consumers' personal freedom could be endangered if the illegitimate processing of personal data leads to judgements about them that exclude them from offerings and services; this issue becomes particularly serious if the data is also shared with third parties (i.e. creditors).

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 14: Retail PIA – Definition of protection demand categories for P2.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P3.1	Legitimacy of processing sensitive personal data	-	-	-	-	-	---

Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.

Table 15: Retail PIA – Definition of protection demand categories for P3.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.1	Providing adequate information in cases of direct collection of data from the data subject	2	2	1	1	2	2

This privacy target is strongly related to P1.1, thus a similar analysis is used.

Retailers know from experience that it is important to take consumers seriously and give them choices. For this purpose, retailers should inform consumers if data is collected from them and processed.

If the data processing activities related to the system landscape are not made transparent to consumers, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if consumers are misinformed (i.e. by call-centre employees, shop employees) or if consumers misjudge the degree of personal data processing involved in the services. A lack of transparency can also lead to limited or contradictory information being picked up by journalists. Finding out about more data processing and use taking place than expected can lead consumers to feel betrayed. In particular, negative press resulting from a lack of transparency is a danger for a company's reputation.
- the operator's financial loss can be considerable when a lack of transparency leads to negative press, consumer backlash, or both. Consumers may avoid visiting retail stores. Image campaigns may be necessary to restore consumers' faith. Stock market valuation can suffer (at least in the short term) when unlawful processing becomes known to the public.
- consumers' reputation can be adversely affected if, without their prior knowledge, information about their purchases and service-use are used for judgements about them (i.e. concerning their creditworthiness, etc.).
- consumers' financial well-being can be adversely affected if, without their prior knowledge, information about their purchases and service-use is used so segment them into groups that disallow access to financially advantageous offerings (i.e. coupons or discounts only accessible to consumers with certain traits).
- consumers' personal freedom could be endangered because they decide to participate in a service, but base this decision on limited or inadequate information about the data processing activities involved.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 16: Retail PIA – Definition of protection demand categories for P4.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 17: Retail PIA – Definition of protection demand categories for P4.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.1	Facilitating the provision of information about processed data and purpose	1	1	1	1	1	1

The retailer strives to communicate openly and transparently with his consumers (see P1.1).

If no information about processed data (i.e. in the form of data categories and items) and purpose is provided to the consumers, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because only a few consumers will probably enforce their legal rights and force the operator to provide a detailed overview of their individual data being processed.
- the operator's financial loss can be acceptable because generating detailed data processing reports for some consumers might not be too costly.
- consumers' reputation cannot be affected significantly.
- consumers' financial well-being cannot be affected significantly.
- consumers' personal freedom cannot be endangered because no data is processed that is so sensitive that it would affect a consumer's freedom. A lack of information thereof or access to it does not limit freedom either.

As all of the criteria are evaluated as being low, the overall evaluation is “low – 1”.

Table 18: Retail PIA – Definition of protection demand categories for P5.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.2	Facilitating the rectification, erasure or blocking of data	1	2	1	1	1	2

This privacy target is strongly related to P1.4, as consumer actions to correct or erase their data will often be triggered by poor data quality. As the quality of services strongly depends on the accuracy of the original and aggregated data, the operator should invest in measures that ensure data quality. Consumers' own rectifications are one way to do so.

If consumers are not enabled to rectify, erase or block their personal data, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because only a few consumers will probably want to correct their data with the operator or ask for erasure and blocking of their data; however, consumers may take such actions in cases where the operator uses poor quality data and engages in senseless consumer communication or when the consumer has a strong desire to not be included in the data sets (i.e. for privacy reasons).
- the operator's financial loss can be considerable if consumers who are not allowed control over their data engage in legal trials. Consumers may also feel put off by poor communication quality with the operator if they cannot impede or de-register from services.
- consumers' reputation can be adversely affected if they are treated (i.e. by an operator's call-centre or retail staff) in a manner that isn't in line with their loyalty track record and if they have no means to correct their data or category.
- consumers' financial well-being can be adversely affected if they do not receive the discounts or advantages that are appropriate for their category or are not able to correct their data or category.
- consumers' personal freedom cannot be endangered because no data is processed that is so sensitive that it would implicate a consumer's freedom.

As one of the criteria is evaluated as being medium, the overall evaluation is “medium – 2”.

Table 19: Retail PIA – Definition of protection demand categories for P5.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 20: Retail PIA – Definition of protection demand categories for P5.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	1	1	1	1	2	2

The retailer clearly and openly communicates the workings of the personalised services he offers, including direct marketing purposes. Consumers should be able to de-register from these services at any time.

If consumers are not enabled to object to the processing of their personal data (e.g. for direct marketing purposes or disclosure to third parties), the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because only a few consumers will probably want to object to processing or direct marketing activities. However, some consumers may be put off if they cannot object to such activities.
- the operator's financial loss can be acceptable because few consumers will probably want to engage in a legal trial to enforce their right to drop out of data processing and direct marketing.
- consumers' reputation cannot be affected significantly.
- consumers' financial well-being cannot be affected significantly.
- consumers' personal freedom is endangered if they cannot exercise their right to informational self-determination on a relatively large scale. The offerings made to them by third parties or direct marketers may limit their options, lead to false judgements, etc. and they may not have any means to stop this. Once the data has been shared,

consumers have no means to get it back.

As one of the criteria is evaluated as being medium, the overall evaluation is “medium – 2”.

Table 21: Retail PIA – Definition of protection demand categories for P6.1

Privacy target code and name		**Criteria for the classification of protection demand categories**					**Overall category**
		Operator perspective		**Consumer perspective**			
		Impact on Reputation and Brand Value	**Financial loss**	**Social standing, reputation**	**Financial well-being**	**Personal freedom**	
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	1	1	1	1	1	1

This privacy target is strongly related to P6.1, thus a similar analysis is used.

The retailer clearly and openly communicates the workings of the services that are based on automated decisions. Consumers can de-register from these services at any time.

If consumers are not enabled to object to being subject to automated decisions, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because only a few consumers will probably want to object to the automated decisions. However, some consumers may be put off if they cannot object to such activities.
- the operator's financial loss can be acceptable because few consumers will probably want to engage in a legal trial to enforce their right to drop out of automated decisions taking place.
- consumers' reputation cannot be affected significantly.
- consumers' financial well-being cannot be affected significantly.
- consumers' personal freedom cannot be endangered. Even though the operator may come to false conclusions based on automated decision making, consumers always have the ability to drop out of the service relationship.

As all of the criteria are evaluated as being low, the overall evaluation is “low – 1”.

Table 22: Retail PIA – Definition of protection demand categories for P6.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P7.1	Safeguarding confidentiality and security of processing	-	-	-	-	-	---
BSI's TG 03126-4 needs to be considered.							

Table 23: Retail PIA – Definition of protection demand categories for P7.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Consumer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P8.1	Compliance with notification requirements	2	2	-	-	-	2
If the operator does not comply with the legally specified notification requirements, the operator may face the following consequences: - the operator's reputation can be considerably impaired because he might get into conflict with the supervisory data protection authority. These conflicts might be exposed to the public. - the operator's financial loss can be considerable if he is forced to pay fines, create the necessary documentation ad-hoc with the help of costly consultants and be subject to regular controls by the supervisory authority in the future. As all of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.							

Table 24: Retail PIA – Definition of protection demand categories for P8.1

2.2.4 Step 4: Identification of relevant threats

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			operator.		
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	y	
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	y	
		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.	y	
		T1.5	Existing information describing the service is not kept up-to-date.	y	
		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.	y	
	Lack of transparency – Missing or insufficient privacy statement	T1.7	No privacy statement is available.	y	
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	y	
		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.	y	
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	y	
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	n	Consumer data is not given to third parties, thus this threat does not apply.
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	y	
	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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			collection process.		
		T1.14	No RFID emblem is displayed on the product and the product packaging.	y	
	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.	y	
		T1.16	The data collection purpose is not documented in an adequate way.	y	
		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.	y	
	Collection and/or combination of data exceeding purpose	T1.18	Collected data is processed for other purposes than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	y	
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	y	
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	y	This threat is related to TV11 “Unauthorised collection and storage of data” ([BSI2008], p. 90).
		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.	y	This threat is related to TV4 “Unauthorised scanning of sales and in-voicing information” and TV11 “Unauthorised collection and storage of data” ([BSI2008], p. 90).
		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.	y	This threat is related to TV12 “Unauthorised linking of data” ([BSI2008], p. 90).
		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	y	This threat is related to TT10 “Tracking by means of unauthorised scanning by third parties”, TT14

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			protection.		"Unauthorised scanning of personal data"and TT15 "Unauthorised writing / manipulation of personal data" ([BSI2008], p. 85-86).
	Missing quality assurance of data	T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	y	
		T1.25	The identification of the data subject is not conducted thoroughly.	y	This threat is related to TV10 "Falsification of identity data" ([BSI2008], p. 90).
		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.	y	
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	y	
	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.	y	
		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.	y	
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.	y	
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	y	
		T2.3	The relevant legal basis (e.g. consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.	y	
T3	Invalidation or non-existence of explicit consent	T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	n	This threat belongs to P3.1, which was excluded from further consideration in

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
					step 2.
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
		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.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
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: - 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.	y	
		T4.2	The relevant information is not provided in an adequate form (e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	y	
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	y	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: - 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?),	n	This threat belongs to P4.2, which was excluded from further consideration in step 2.

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			- the existence of the right of access to and the right to rectify the data concerning him.		
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	n	This threat belongs to P4.2, which was excluded from further consideration in step 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.	n	This threat belongs to P4.2, which was excluded from further consideration in step 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.	y	
		T5.2	Access is possible but not to all relevant data, including: - 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.	y	
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	y	This threat is related to TV8 “Unauthorised scanning of personal data” and TV10 “Falsification of identity data” ([BSI2008], p. 90).

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		T5.4	Successful access as well as subsequent data disclosure is not logged.	y	
	Inability to rectify, erase or block individual data	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.	y	
		T5.6	Errors are not automatically rectified.	y	
		T5.7	There is no procedure that allows the erasure of individual data in back-up data.	y	
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	y	This threat is related to TV7 “Unauthorised writing / manipulating of sales and invoicing information”, TV9 “Unauthorised writing / manipulation of personal data” and TV10 “Falsification of identity data” ([BSI2008], p. 90).
		T5.9	Successful rectification, erasure and blocking is not logged.	y	
	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.	n	This threat belongs to P5.3, which was excluded from further consideration in step 2.
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.	y	
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	y	
		T6.3	The operator has not implemented any procedure that would allow the notification of relevant third parties in the case that a data subject has objected to the processing of his personal data.	n	Consumer data is not handed over to third parties, thus this threat does not apply.
	Inability to allow objection to being subject to decisions that are solely	T6.4	The data subject cannot object to automated decision procedures that are used in the realm of the offered service.	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
	based on automated processing of data				
T7	Refer to security-relevant threats that are defined in BSI's technical guidelines TG 03126-4.	T7.1	Refer to the description of security-relevant threats that are defined in BSI's technical guidelines TG 03126-4.	y	BSI's TG 03126-4 needs to be considered.
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.	y	
		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.	y	
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	y	
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	y	

Table 25: Retail PIA – Identification of relevant threats

2.2.5 Step 5: Identification and recommendation of controls

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.1	C1.1	SERVICE DESCRIPTION	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.
	C1.4	INFORMATION TIMELINESS		The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
	C6.2	HANDLING OBJECTIONS TO AUTOMATED DECISIONS		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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				are disabled on request.
T1.2	C1.2	INFORMATION ACCESSIBILITY	2 (P1.1)	The information describing the service is made accessible at the operator's physical facilities and online.
T1.3	C1.1	SERVICE DESCRIPTION	2 (max of P1.1 and P1.2)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.
T1.4	C1.1 C1.3	SERVICE DESCRIPTION LANGUAGE / SEMANTICS OF INFORMATION	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. 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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
T1.5	C1.4	INFORMATION TIMELINESS	2 (P1.1)	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.6	C1.1 C1.2	SERVICE DESCRIPTION INFORMATION ACCESSIBILITY	2 (max of P1.1 and P1.2)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The information describing the service is made accessible at the operator's physical facilities and online.
T1.7	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.8	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.9	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.10	C1.5	PRIVACY STATEMENT	2 (P1.1)	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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				operator.
T1.12	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.13	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.14	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.15	C1.7	PURPOSE SPECIFICATION	2 (P1.2)	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.
T1.16	C1.7	PURPOSE SPECIFICATION	2 (max of P1.1 and P1.2)	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.
T1.17	C1.8	ENSURING LIMITED DATA PROCESSING	2 (P1.2)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.
T1.18	C1.8 C1.9	ENSURING LIMITED DATA PROCESSING ENSURING PURPOSE RELATED PROCESSING	2 (P1.3)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level. 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.
T1.19	C1.9	ENSURING PURPOSE RELATED PROCESSING	2 (P1.3)	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.
T1.20	C1.10	ENSURING DATA	2	Data collection is regularly checked under the aspect of data

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
		MINIMISATION	(max of P1.3 and TV11 ([BSI2008], p. 136))	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. Related safeguard from [BSI2008]: **MV2** "Satisfying the data minimisation obligation": "Satisfying legal requirements: - When the processes and system within the overall system are being defined, the principle of data minimisation is applied in accordance with the legal foundations. This includes, in particular, the definition of deadlines for deleting data that is no longer required." (p. 116)
T1.21	C1.10	ENSURING DATA MINIMISATION	3 (max of P1.3 and TV4 and TV11 ([BSI2008], p. 136))	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguards from [BSI2008]: **MS6** "Confidential storage of data": "Introduction of multi-tenant access protection: - Only a certain, legitimised group of people can access stored data (personal data, sales data, usage data, invoicing data, blacklists, approval lists, etc.). - Data is stored in an environment protected against unauthorised access. If access protection cannot be guaranteed, then the data should be stored on an encrypted data carrier (hard drive encryption tools are used). Alternatively, other equally effective encryption mechanisms can be used. The algorithm strength must be at least that of the 3DES algorithm. The type and strength of the mechanism should be adapted to future developments in accordance with[ALGK_BSI]. Introduction of multi-tenant access protection with a defined role model. - A client concept in the form of a role model is to be established." (p. 94)

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				MV2 “Satisfying the data minimisation obligation”: “Satisfying legal requirements: - When the processes and system within the overall system are being defined, the principle of data minimisation is applied in accordance with the legal foundations. This includes, in particular, the definition of deadlines for deleting data that is no longer required. Special safeguards - Precise, purpose-related definition of the data content, the acquisition and storage of data, and access and usage rights using the role model of the overall system. - The customer is informed about the purpose-related acquisition, storage and use of personal data.” (p. 116)
T1.22	C1.8	ENSURING LIMITED DATA PROCESSING	3 (max of P1.3 and TV12 ([BSI2008], p. 137))	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather fine-grained level. Related safeguard from [BSI2008]: **MV3** “Separation of personal data and logistical data”: “The allocation of personal customer data to information about the objects fitted with transponders is only permitted with the express approval of the customer and for a defined purpose. Implementing the separation of personal data and logistical data Special safeguards - The customer is informed about the content of the logistical data used, the way in which it is linked to personal data, the purpose for which it is used, and the length of time for which it will be stored and used. - The customer is informed about the purpose-related acquisition, storage, duration of storage and use of personal data. - This implementation requires the customer's agreement.” (p. 116)
T1.23	C1.11	ENSURING TAG PROTECTION	2 (max of P1.3 and TT10 ([BSI2008], p. 162))	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguards from [BSI2008]: **MT10** “Preventing the generation of movement profiles”: “According to current specifications, EPC chips can include a

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				command (the kill command) which irreversibly deactivates the chip. For this reason, the safeguard below is currently stipulated by EPCglobal in reference implementations for all protection demand categories. Other proprietary methods are conceivable, these being similarly suitable for preventing the generation of movement profiles. These, however, have not yet been specified by EPCglobal and implemented in the EPC chips. Preventing retrieval of data from the transponder - Deactivate the transponder using the kill command when the tagged product is sold, or use a similarly secure technical method." (p. 104-105) **MT11** "Preventing the assignment of movement profiles to people": "The tracking of a transponder after it has been given to the customer is only to be considered a threat if the movement profile can be linked to a particular person. It should be noted that from a large volume of anonymous movement data that has been suitably aggregated, data can be generated that can be, or in some cases already is, related to particular people. Guaranteed anonymity of sale: - Anonymous sale and handing-over of the product to the customer (anonymous payment procedure, no use of discount or customer cards, no product delivery). - General ban on linking products and personal data in retailers' IT systems. This also applies when customer cards are used. Certification: - The implementation of these safeguards is also checked and certified by an independent authority." (p. 105)
T1.24	C1.12	ENSURING PERSONAL DATA QUALITY	2 (P1.4)	Data collection forms and tools are designed and implemented in such a way that completeness and correctness of the data can be ensured in the best possible way.
T1.25	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3 (max of P1.4 and TV10 ([BSI2008], p. 136))	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online. Related safeguard from [BSI2008]: **MV1** "Identifying the customer when selling and handing over products": "The identity of the customer must be established when setting up a customer account and when delivering or collecting products.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				Identity document check when setting up a customer account and issuing a customer card: - Secure photo ID is presented. - The identity data is taken into the system from a secure electronic identity card (eID).” (p. 115-116)
T1.26	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	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.
T1.27	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	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.
T1.28	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T1.29	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T2.1	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.2	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.3	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T4.1	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.2	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.3	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- 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.
T5.1	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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.
T5.2	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- the logic involved in any automatic processing of data and automated decisions. 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.
T5.3	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3 (max of P5.1 and TV8, TV10 ([BSI2008], p. 136))	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online. Related safeguards from [BSI2008]: **MS5** "Securing the confidentiality of data when communicating within the system": "Encryption for internal communication: - Data is transmitted in encrypted form. Alternatively, instead of general data encryption, data can be sent via dedicated networks (closed solution), in which only authorised users are administered and allowed. This network would need to be protected against physical attacks from the outside by means of appropriate safeguards (e.g. basic protective measures), and then operated in accordance with an appropriate security concept. Secure communication channel: - Communication between the components of the system is via VPNs or a similar (shielded) solution. Before communication, authentication is performed by negotiating a key between sender and receiver. The negotiated key is then used for communication." (p. 94) **MS6** "Confidential storage of data": "Introduction of multi-tenant access protection: - Only a certain, legitimised group of people can access stored data (personal data, sales data, usage data, invoicing data, blacklists, approval lists, etc.). - Data is stored in an environment protected against unauthorised access. If access protection cannot be guaranteed, then the data should be stored on an encrypted data carrier (hard drive encryption tools are used). Alternatively, other equally effective encryption mechanisms can be used. The algorithm strength must be at least that of the 3DES algorithm.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				The type and strength of the mechanism should be adapted to future developments in accordance with[ALGK_BSI]. Introduction of multi-tenant access protection with a defined role model. - A client concept in the form of a role model is to be established." (p. 94) **MV1** "Identifying the customer when selling and handing over products": "The identity of the customer must be established when setting up a customer account and when delivering or collecting products. Identity document check when setting up a customer account and issuing a customer card: - Secure photo ID is presented. - The identity data is taken into the system from a secure electronic identity card (eID)." (p. 115-116)
T5.4	C5.2	LOGGING ACCESS TO PERSONAL DATA	1 (P5.1)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T5.5	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.6	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.7	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 subject's request. These

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T5.8	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3 (max of P5.2 and TV7, TV9, TV10 ([BSI2008], p. 136))	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online. Related safeguards from [BSI2008]: **MS6** "Confidential storage of data": "Introduction of multi-tenant access protection: - Only a certain, legitimised group of people can access stored data (personal data, sales data, usage data, invoicing data, blacklists, approval lists, etc.). - Data is stored in an environment protected against unauthorised access. If access protection cannot be guaranteed, then the data should be stored on an encrypted data carrier (hard drive encryption tools are used). Alternatively, other equally effective encryption mechanisms can be used. The algorithm strength must be at least that of the 3DES algorithm. The type and strength of the mechanism should be adapted to future developments in accordance with[ALGK_BSI]. Introduction of multi-tenant access protection with a defined role model. - A client concept in the form of a role model is to be established." (p. 94) **MS7** "Securing the data integrity in order to protect against manipulation when transmitting data within the system": "MAC or signatures: - The integrity of data transmission is guaranteed using MAC protection or by signatures. MAC and signature processes are to be chosen in accordance with [ALGK_BSI]. - The type and strength of the mechanism should be adapted to future developments in accordance with [ALGK_BSI]." (p. 94-95) **MS8** "Securing data integrity when storing data": "Data is stored in a secure environment with access protection as defined in MS6. Checksums:

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- A checksum is used to protect against technically related integrity failures (CRC, hamming codes, ...); this can also be provided by the operating system involved." (p. 95) **MV1** "Identifying the customer when selling and handing over products": "The identity of the customer must be established when setting up a customer account and when delivering or collecting products. Identity document check when setting up a customer account and issuing a customer card: - Secure photo ID is presented. - The identity data is taken into the system from a secure electronic identity card (eID)." (p. 115-116)
T5.9	C5.2	LOGGING ACCESS TO PERSONAL DATA	2 (P5.2)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T6.1	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2 (P6.1)	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.
T6.2	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2 (P6.1)	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.
T6.4	C6.2	HANDLING OBJECTIONS TO AUTOMATED DECISIONS	1 (P6.2)	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. They are informed that the automated decisions cannot be disabled and that they are free to deregister from the service.
T7.1	C7.1	SECURITY CONTROLS	--- (P7.1)	See relevant controls from TG 03126-4.
T8.1	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				application's launch.
T8.2	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.
T8.3	C8.2	PRIOR CHECKING	2 (P8.1)	It is ensured that the legally required checking of the RFID application is executed by expert personnel.
T8.4	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.

Table 26: Retail PIA – Identification and recommendation of controls

2.2.5.1 Consolidated view of identified controls

Control code and name		Highest overall category	Description
C1.1	SERVICE DESCRIPTION	2	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.
C1.2	INFORMATION ACCESSIBILITY	2	The information describing the service is made accessible at the operator's physical facilities and online.
C1.3	LANGUAGE / SEMANTICS OF INFORMATION	2	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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
C1.4	INFORMATION TIMELINESS	2	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
C1.5	PRIVACY STATEMENT	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

Control code and name		Highest overall category	Description
			operator.
C1.6	RFID EMBLEM	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.
C1.7	PURPOSE SPECIFICATION	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.
C1.8	ENSURING LIMITED DATA PROCESSING	3	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. Related safeguard from [BSI2008]: **MV3** "Separation of personal data and logistical data": "The allocation of personal customer data to information about the objects fitted with transponders is only permitted with the express approval of the customer and for a defined purpose. Implementing the separation of personal data and logistical data Special safeguards - The customer is informed about the content of the logistical data used, the way in which it is linked to personal data, the purpose for which it is used, and the length of time for which it will be stored and used. - The customer is informed about the purpose-related acquisition, storage, duration of storage and use of personal data. - This implementation requires the customer's agreement." (p. 116)
C1.9	ENSURING PURPOSE RELATED PROCESSING	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.
C1.10	ENSURING DATA MINIMISATION	3	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see

Control code and name		Highest overall category	Description
			Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguards from [BSI2008]: **MS6** "Confidential storage of data": "Introduction of multi-tenant access protection: - Only a certain, legitimised group of people can access stored data (personal data, sales data, usage data, invoicing data, blacklists, approval lists, etc.). - Data is stored in an environment protected against unauthorised access. If access protection cannot be guaranteed, then the data should be stored on an encrypted data carrier (hard drive encryption tools are used). Alternatively, other equally effective encryption mechanisms can be used. The algorithm strength must be at least that of the 3DES algorithm. The type and strength of the mechanism should be adapted to future developments in accordance with[ALGK_BSI]. Introduction of multi-tenant access protection with a defined role model. - A client concept in the form of a role model is to be established." (p. 94) **MV2** "Satisfying the data minimisation obligation": "Satisfying legal requirements: - When the processes and system within the overall system are being defined, the principle of data minimisation is applied in accordance with the legal foundations. This includes, in particular, the definition of deadlines for deleting data that is no longer required. Special safeguards - Precise, purpose-related definition of the data content, the acquisition and storage of data, and access and usage rights using the role model of the overall system. - The customer is informed about the purpose-related acquisition, storage and use of personal data." (p. 116)
C1.11	ENSURING TAG PROTECTION	2	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguards from [BSI2008]: **MT10** "Preventing the generation of movement profiles": "According to current specifications, EPC chips can include a

Control code and name		Highest overall category	Description
			command (the kill command) which irreversibly deactivates the chip. For this reason, the safeguard below is currently stipulated by EPCglobal in reference implementations for all protection demand categories. Other proprietary methods are conceivable, these being similarly suitable for preventing the generation of movement profiles. These, however, have not yet been specified by EPCglobal and implemented in the EPC chips. Preventing retrieval of data from the transponder - Deactivate the transponder using the kill command when the tagged product is sold, or use a similarly secure technical method." (p. 104-105) **MT11** "Preventing the assignment of movement pro- files to people": "The tracking of a transponder after it has been given to the customer is only to be considered a threat if the movement profile can be linked to a particular person. It should be noted that from a large volume of anonymous movement data that has been suitably aggregated, data can be generated that can be, or in some cases already is, related to particular people. Guaranteed anonymity of sale: - Anonymous sale and handing-over of the product to the customer (anonymous payment procedure, no use of discount or customer cards, no product delivery). - General ban on linking products and personal data in retailers' IT systems. This also applies when customer cards are used. Certification: - The implementation of these safeguards is also checked and certified by an independent authority." (p. 105)
C1.12	ENSURING PERSONAL DATA QUALITY	2	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.
C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online. Related safeguard from [BSI2008]: **MS5** "Securing the confidentiality of data when communicating within the system": "Encryption for internal communication: - Data is transmitted in encrypted form. Alternatively, instead of general data encryption, data can be sent via dedicated networks (closed solution), in which only

Control code and name		Highest overall category	Description
			authorised users are administered and allowed. This network would need to be protected against physical attacks from the outside by means of appropriate safeguards (e.g. basic protective measures), and then operated in accordance with an appropriate security concept. Secure communication channel: - Communication between the components of the system is via VPNs or a similar (shielded) solution. Before communication, authentication is performed by negotiating a key between sender and receiver. The negotiated key is then used for communication." (p. 94) **MS6** "Confidential storage of data": "Introduction of multi-tenant access protection: - Only a certain, legitimised group of people can access stored data (personal data, sales data, usage data, invoicing data, blacklists, approval lists, etc.). - Data is stored in an environment protected against unauthorised access. If access protection cannot be guaranteed, then the data should be stored on an encrypted data carrier (hard drive encryption tools are used). Alternatively, other equally effective encryption mechanisms can be used. The algorithm strength must be at least that of the 3DES algorithm. The type and strength of the mechanism should be adapted to future developments in accordance with[ALGK_BSI]. Introduction of multi-tenant access protection with a defined role model. - A client concept in the form of a role model is to be established." (p. 94) **MS7** "Securing the data integrity in order to protect against manipulation when transmitting data within the system": "MAC or signatures: - The integrity of data transmission is guaranteed using MAC protection or by signatures. MAC and signature processes are to be chosen in accordance with [ALGK_BSI]. - The type and strength of the mechanism should be adapted to future developments in accordance with [ALGK_BSI]." (p. 94-95) **MS8** "Securing data integrity when storing data": "Data is stored in a secure environment with access protection as defined in MS6. Checksums:

Control code and name		Highest overall category	Description
			- A checksum is used to protect against technically related integrity failures (CRC, hamming codes, ...); this can also be provided by the operating system involved." (p. 95) **MV1** "Identifying the customer when selling and handing over products": "The identity of the customer must be established when setting up a customer account and when delivering or collecting products. Identity document check when setting up a customer account and issuing a customer card: - Secure photo ID is presented. - The identity data is taken into the system from a secure electronic identity card (eID)." (p. 115-116)
C1.14	ENSURING DATA ACCURACY	2	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.
C1.15	ENABLING DATA DELETION	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.
C2.1	OBTAINING DATA SUBJECT'S CONSENT	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.
C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2	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 might be accessible online via a

Control code and name		Highest overall category	Description
			link on the data collection form / tool and that leads to a separate web page that contains legal information.
C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1	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: - 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. 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.
C5.2	LOGGING ACCESS TO PERSONAL DATA	2	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2	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 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.
C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2	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.
C6.2	HANDLING OBJECTIONS TO AUTOMATED DECISIONS	2	The logic involved in any automatic processing of data and automated decisions is described and made available to the

Control code and name		Highest overall category	Description
			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.
C7.1	SECURITY CONTROLS	---	See relevant controls from TG 03126-4.
C8.1	NOTIFICATION OF AUTHORITY	2	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 weeks prior to the RFID application's launch.
C8.2	PRIOR CHECKING	2	It is ensured that the legally required checking of the RFID application is executed by expert personnel.

Table 27: Retail PIA – Consolidated view of identified controls

2.2.6 Step 6: Documentation of residual risks

For technical or business reasons it is not always possible to eliminate threats completely by applying controls. Some residual risks remain. These residual risks should be documented in this step. It is recommended to provide a comprehensive description and an evaluation (low, medium, high) for each residual risk.

3 Public Transport Scenario

3.1 Initial analysis

For the initial analysis, the decision tree shown in Figure 1 is used. For the current scenario, the answer to Q1 is: Yes, the RFID application does process personal data. Personal data is stored and processed in personalised user accounts and profiles in the ticket management system and the added-value service management system.

The answer to Q2a is open to some interpretation: If the answer is based solely on the definition of personal data in the Directive 95/46/EC, RFID tags used in the application do not contain personal data. Consequently, the resulting level of PIA analysis is 2 and a full scale PIA is required. If, however, the answer to this question is based on the definition of personal data from Directive 95/46/EC **as well as** WP 136 [ART2007] and WP 175 [ART2010], then RFID tags used in the application do contain personal data. This is the case for personalised tickets as well as for non-personalised tickets. Thus, the resulting level is 3 and a full scale PIA is required.

Both answers to Q2a require a full scale PIA.

3.2 Risk assessment

The following description of a risk assessment is an exemplary execution of a PIA. A PIA that is conducted by a different group of stakeholders may lead to different conclusions. In particular, the context descriptions and examples in step 2, as well as the reasoning used to derive the demand categories in step 3, might be subjective and are a result of the discussions of the participating stakeholder group. Again, another stakeholder group may come up with different and additional damage scenarios and potential implications. The aim of a PIA is to create a common understanding about the RFID application's privacy implications within the involved stakeholder group and thus facilitates commonly accepted conclusions.

3.2.1 Step 1: Characterisation of the application

3.2.1.1 Systems and entities

3.2.1.1.1 Systems and system components

Figure 33 gives a generic overview regarding the systems and their associated components that form the backend system, which is required to realize the described public transport scenario. Most likely, the different systems will reside on different locations and will be under the responsibility of different entities. This is indicated in Figure 33 by grouping the systems and their components accordingly.

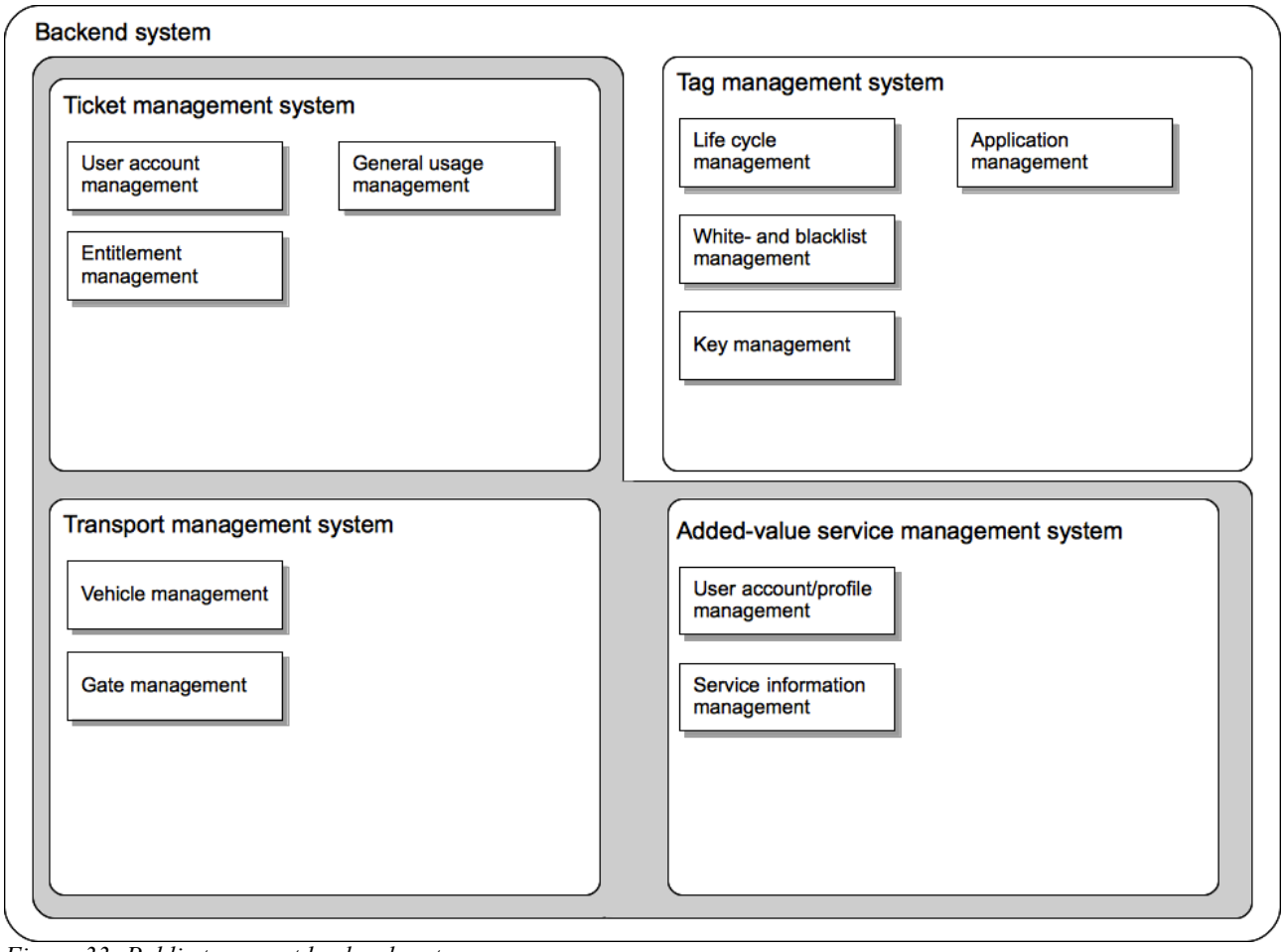

Figure 33: Public transport backend system

The ticket management system provides all functions and processes that are needed for customer and user management, ticket and entitlement management, service usage analysis and the like. It consists of three main components:

- User account management
  This component provides all necessary functions to create, update and delete user accounts. The account is personalised and contains a customer's personal data, e.g. name and address, as well as payment information if the customer chose monthly billing or special best price offers. Additionally, it contains data concerning check-in and -out of public transport vehicles and gates, e.g. to enable monthly best price billing.
- Entitlement management
  This component provides all necessary functions to manage the different types of entitlements that are offered by the public transport operator. Amongst other information, it provides detailed entitlement descriptions, contract details and required payment options for each type of entitlement.
- General usage management
  This component provides all necessary functions to gather and analyse data that describes the usage of the operator's facilities and vehicles. E.g. check-in and -out data that is created through the usage of non-personalised tickets is gathered here. This can later be combined with the check-in and -out data of the personalised user accounts to analyse general usage patterns and the like.

The transport management system provides the functions and processes that deal with vehicle and facility management. The following two main components are relevant for the described scenario:

- Vehicle management
  This component provides all necessary functions to manage the whereabouts, timeliness, working status of the operator's vehicles.
- Gate management
  This component provides all necessary functions to manage the working status of the static gates and facilities.

As there are different carrier mediums utilized throughout the described public transport scenario, these are summarized under the term “tag”. In the detailed use case descriptions, the term “tag” is then specified with prefixes, e.g. ticket tag.

The tag management system provides the functions and processes that are needed to manage the tags regardless of the relevant carrier medium. It consists of four main components:

- Life cycle management
  This component provides all necessary functions to personalise, configure and change the tag with the contact-less interface.
- White- and blacklist management
  This component provides all necessary functions to provide, update and distribute white- and blacklists of tags as well as applications.
- Key Management
  This component encloses all relevant security parameters and cryptographic keys. Key management procedures work as described in 7.12 of [BSI2010].
- Application Management
  This component provides all necessary functions to provide, update and withdraw applications.

The added-value service management system is operated by a service provider and deals with the provision of an added-value service. It consists of two main components:

- User account/profile management
  This component provides all necessary functions to create, update and delete user accounts. These accounts are always personalised as they link to the customer's mobile device. Additionally, the account contains a customer's preferences, travel plans and the like in form of a profile.
- Service information management
  This component provides all necessary functions to manage the acquisition, structuring and distribution of the service information, e.g. time schedule changes, construction impacts, personalised travel information.

3.2.1.1.2 Entities and their roles

The following entities have been identified to be relevant for the described public transport scenario:

- Customer
  A person who uses the offered public transport services. Each customer is the holder of a ticket. This ticket might either be a personalised or a non-personalised RFID-enabled card. The customer is identical to the one described in [BSI2009], page 19.

- Public transport service provider
  An organisation that manages public transport facilities and vehicles and offers public transport services. The public transport service provider is identical to the “service provider” described in [BSI2009], page 21.
- Added-value service provider
  An organisation that offers an added-value service that might be useful in connection with public transport services.

3.2.1.2 Generic business processes

3.2.1.2.1 Process T-P1: Registering for and buying a personalised ticket

Public transport operators generally offer the usage of personalised tickets, especially if a customer buys an entitlement that is valid for a year or more.

In order to obtain a personalised ticket the customer needs to provide some personal data to the public transport operator. The amount of personal data that needs to be provided depends on the entitlement type as well as on the payment option, e.g. monthly payments, cash payments. After successful registration, the customer receives a personalised ticket in the form of an RFID-enabled card. This card is personalised with the customer's name, thus the customer's name is printed on the card and the card's technical ID is linked to the customer's personal data in the user account of the ticket management system. The card is then delivered to the customer's home address.

When the customer received his personalised ticket he can buy an entitlement and load it onto the ticket. This can either happen via a web application at home or at a vending machine.

If the customer wants to give up his contract with the public transport operator, the latter offers a de-registration service. The public transport operator asserts, that, when a certain period of time elapsed after the customer has filed the de-registration request, the customer's data will be deleted.

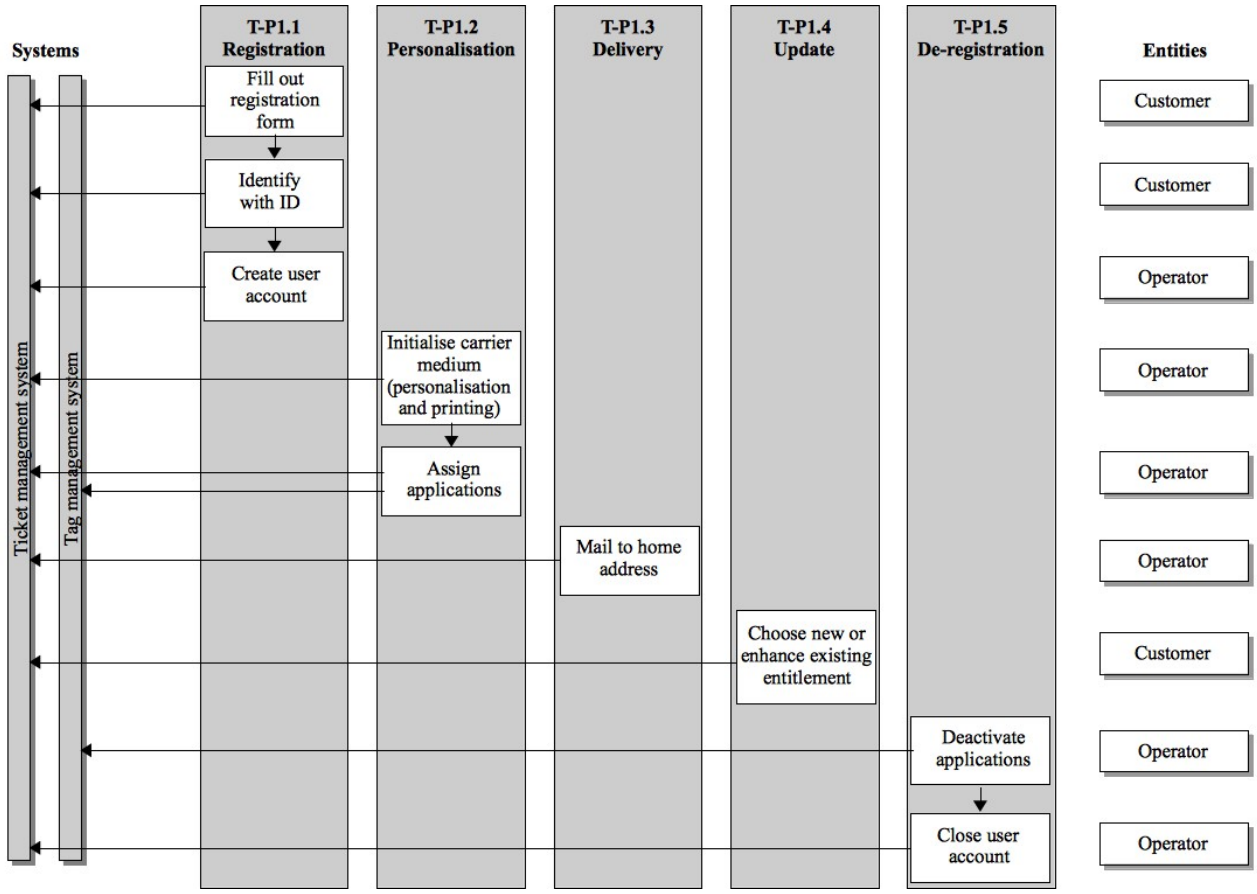

Figure 34: Process T-P1 – Registering for and buying a personalised ticket

3.2.1.2.2 Process T-P2: Registering for and buying a personalised ticket with an existing carrier medium

In addition to the personalised ticket card as described in P1, a public transport operator also offers the usage of a personalised ticket in conjunction with an existing carrier medium. Such an existing carrier medium might be e.g. a multi-application card or an NFC mobile device, which is already in the possession of a customer.

This process is identical to P1, the only difference is, that there is no RFID-enabled card personalised, but the existing carrier medium is initialised (P2.2) so that entitlements can be loaded onto it.

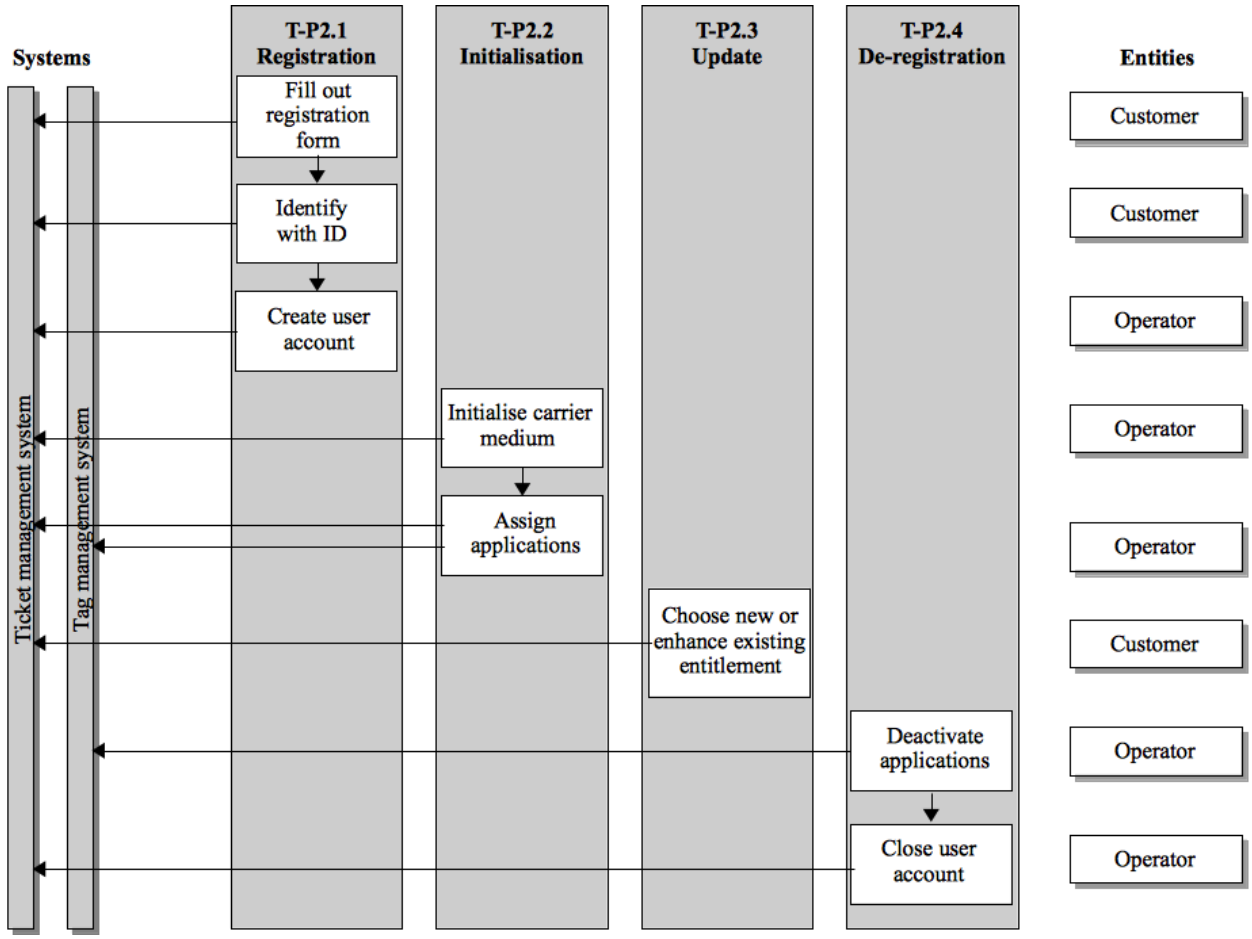

Figure 35: Process T-P2 – Registering for and buying a personalised ticket with an existing carrier medium

3.2.1.2.3 Process T-P3: Buying a non-personalised ticket

In addition to personalised tickets, public transport operators generally offer the usage of non-personalised tickets. These may either be paper tickets or RFID-enabled cards, which are not linked to a distinct person/customer. In the present scenario, the latter option is described.

These non-personalised tickets can be bought for a small amount of money at vending machines or service points. Afterwards, a customer can buy entitlements and load these onto the non-personalised ticket.

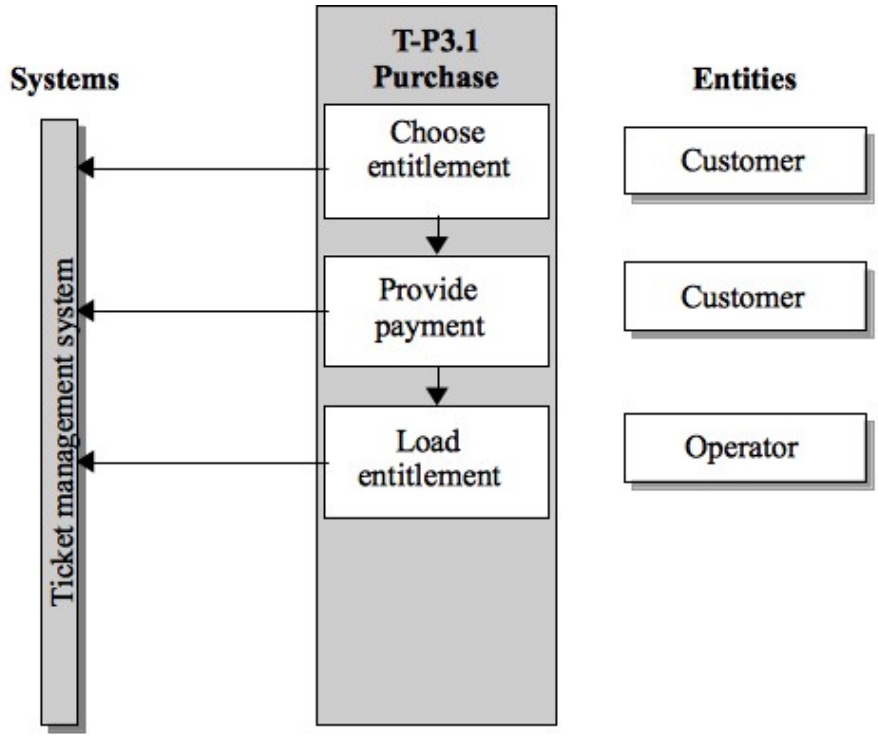

Figure 36: Process T-P3 – Buying a non-personalised ticket

3.2.1.2.4 Process T-P4: Travelling

Public transport facilities and buildings are equipped with static gates that require the customer to provide his ticket. These gates inhibit readers with which the tickets can be read. Additionally, in cases when there are no static gates, public transport vehicles are equipped with readers.

Every time a customer uses the public transport, he needs to check-in and check-out with his ticket at a gate or in the vehicle itself. These check-in and -out events are registered in the ticket management system. They can later be used to compute monthly bills or to facilitate best price models.

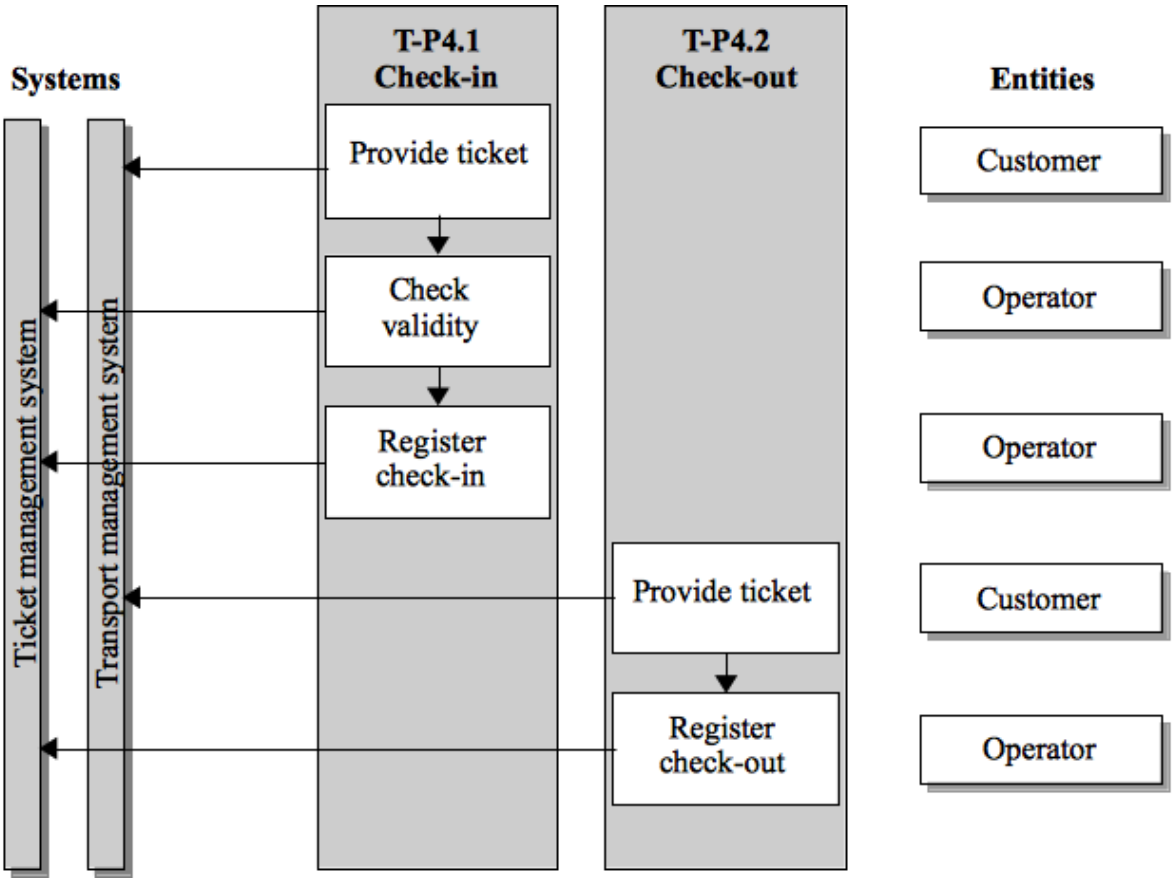

Figure 37: Process T-P4 – Travelling

3.2.1.2.5 Process T-P5: Registering for and using an added-value service

Regular public transport offers might be enhanced with added-value services. These services can either be offered by a specialised service provider or by the public transport operator himself.

An example would be a service that provides information which is relevant during travelling, e.g. time schedule changes, construction impacts, personalised travel information. Additionally, a customer could publish his current location to his friends, so hat they can get information about when and where he will arrive.

Such an added-value service relies on the customer's mobile handheld device. In order to use the service, the customer needs to register his mobile device with the service provider, e.g. load the respective application onto the mobile device. In addition, there is the possibility to store preferences and the like in an online account in the added-value service management system.

Assuming that mobile handheld devices are always personalised, e.g. via the contract with the mobile telecom provider, the described added-value service cannot be used anonymously.

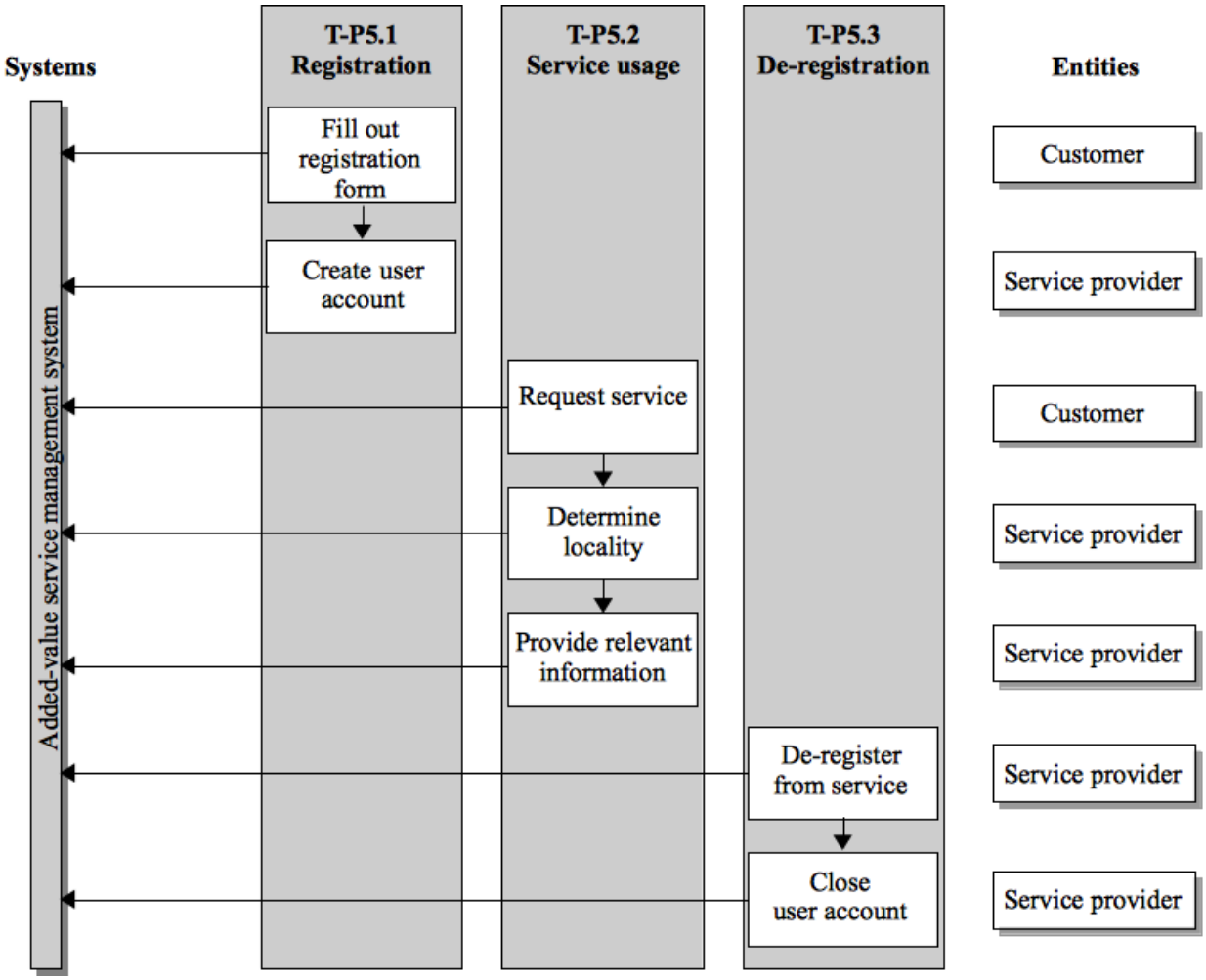

Figure 38: Process T-P5 – Registering for and using an added-value service

3.2.1.3 Use cases

3.2.1.3.1 Use case T-UC 1.1: Registering for a personalised ticket

The customer needs to fill out a registration form to register for a personalised ticket. This can either be done

- via a piece of paper
  In this case, the service person who receives the paper form from the customer checks if all personal data that is necessary to register has been provided by the customer. Additionally, he checks the customer's ID to ensure that the name on the form and the customer are identical.
- or via a web application
  In this case, the application ensures that all necessary personal data has been provided by the customer. The customer proves his identity by providing his eID to the application.

The registration form is then processed and a user account containing the customer's personal data is created in the ticket management system.

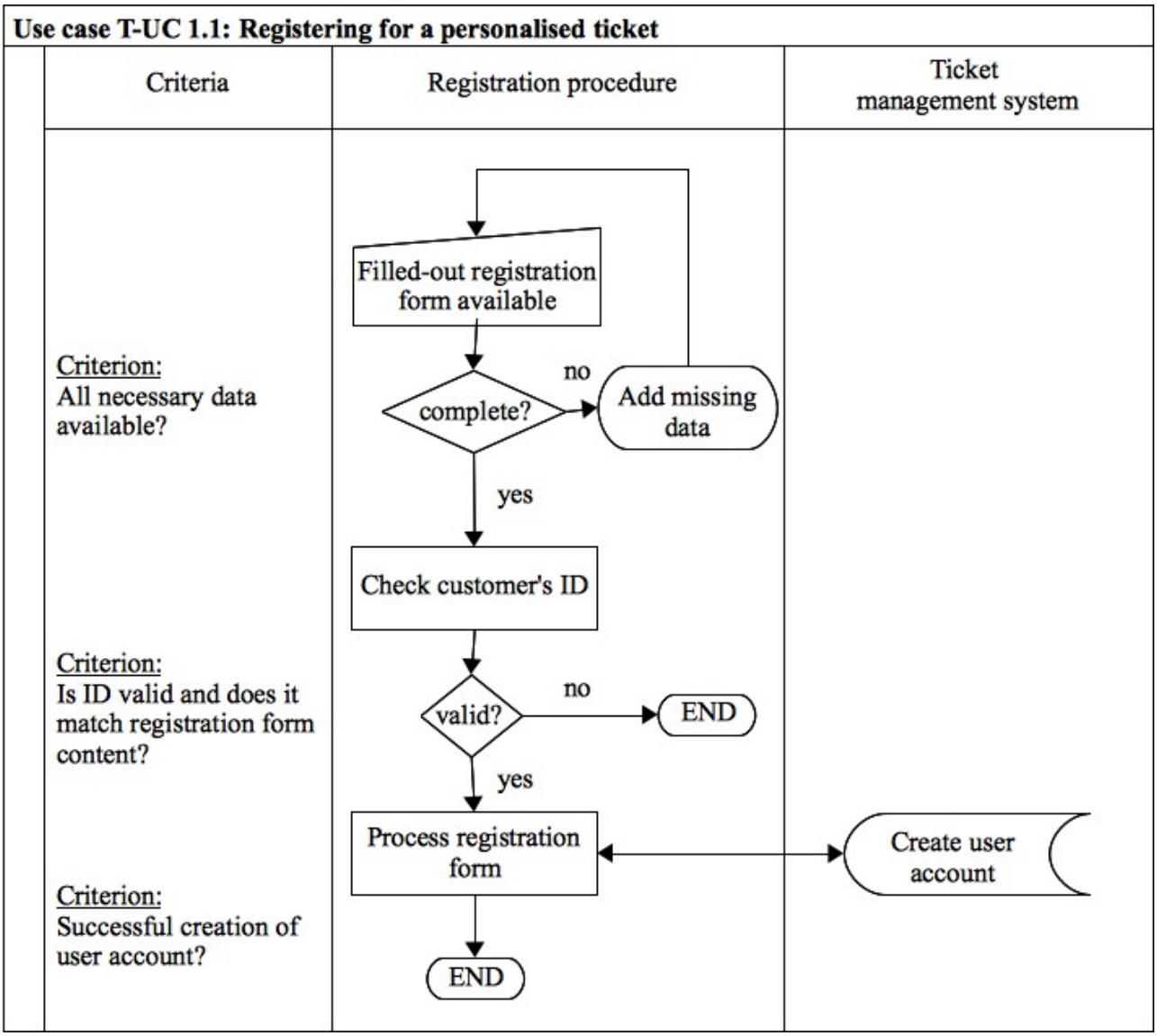

Figure 39: Use case T-UC 1.1 – Registering for a personalised ticket

3.2.1.3.2 Use case T-UC 1.2: Personalising a ticket

The order request for a personalised ticket is processed by the ticket management system. A new ticket is initialised with an ID and this ID is then registered in the respective user account. If there is the need for distinct card applications, these are initialised and registered in the user account, too. Finally, the customer's name and/or his photo are printed onto the (ticket) card.

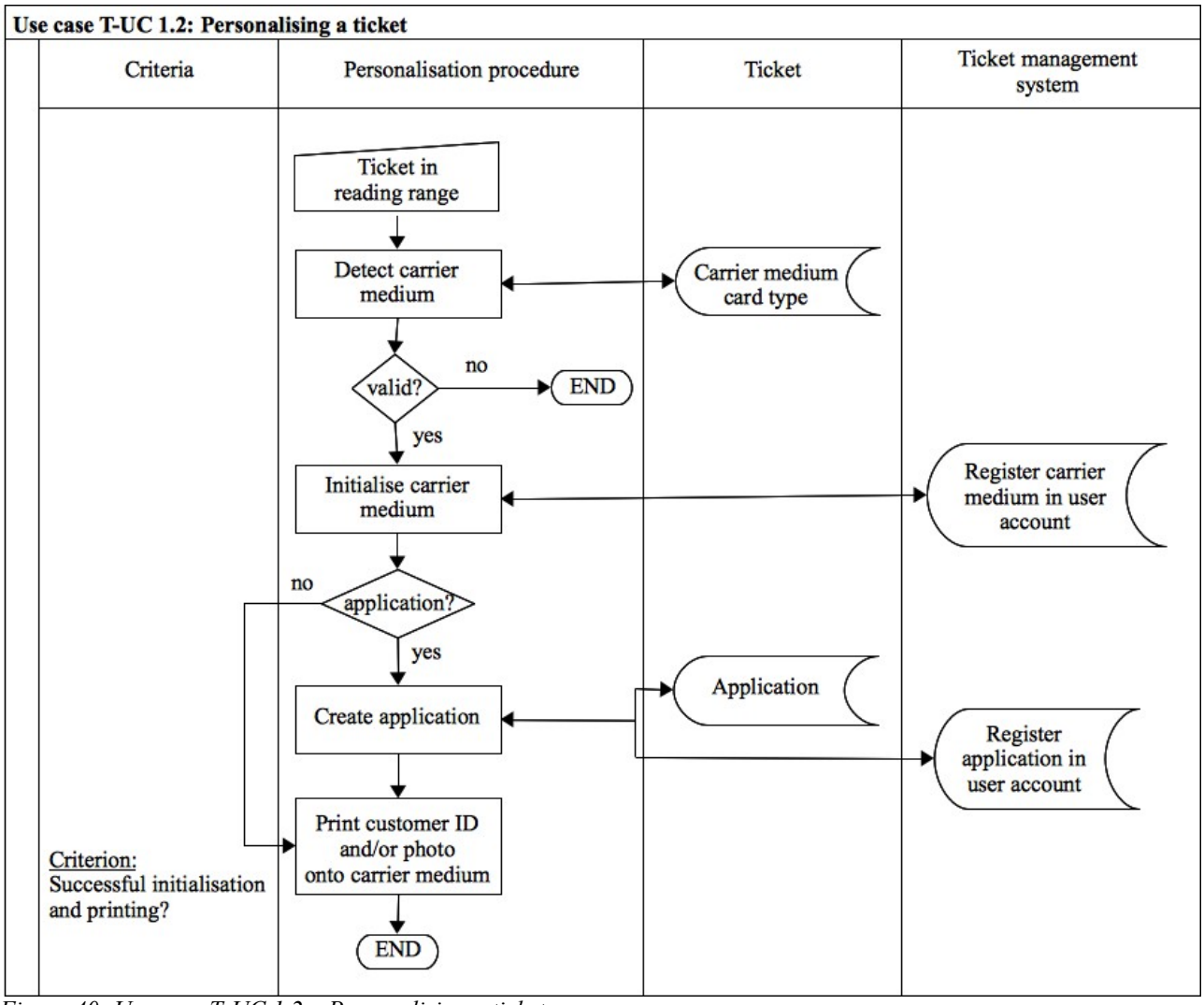

Figure 40: Use case T-UC 1.2 – Personalising a ticket

3.2.1.3.3 Use case T-UC 1.3: Delivering a personalised ticket

The personalised ticket is then mailed to the customer's home address.

3.2.1.3.4 Use case T-UC 1.4: Updating the entitlement on a personalised ticket

After having received his personalised ticket, the customer can buy an entitlement and load it onto the ticket. This can either happen via a web application at home or at a vending machine.

The customer first needs to hold his ticket in front of the reader. A medium and application authentication follows; for a detailed description of this authentication step see figure 7-3 in [BSI2009], page 44. He is then offered an overview of entitlements that he can purchase. When he chooses a specific entitlement it is checked what payment options are available. Depending on the entitlement and the payment preferences in the user's account, the customer can either pay cash or via monthly bills. If he is allowed and decides to pay cash, the payment transaction is performed. If the customer decides for the monthly bill option, the procedure directly continues with the loading

of the entitlement onto the ticket. Additionally, an entitlement entry is written to the user account, which describes e.g. the entitlement type and its validity time frame if necessary.

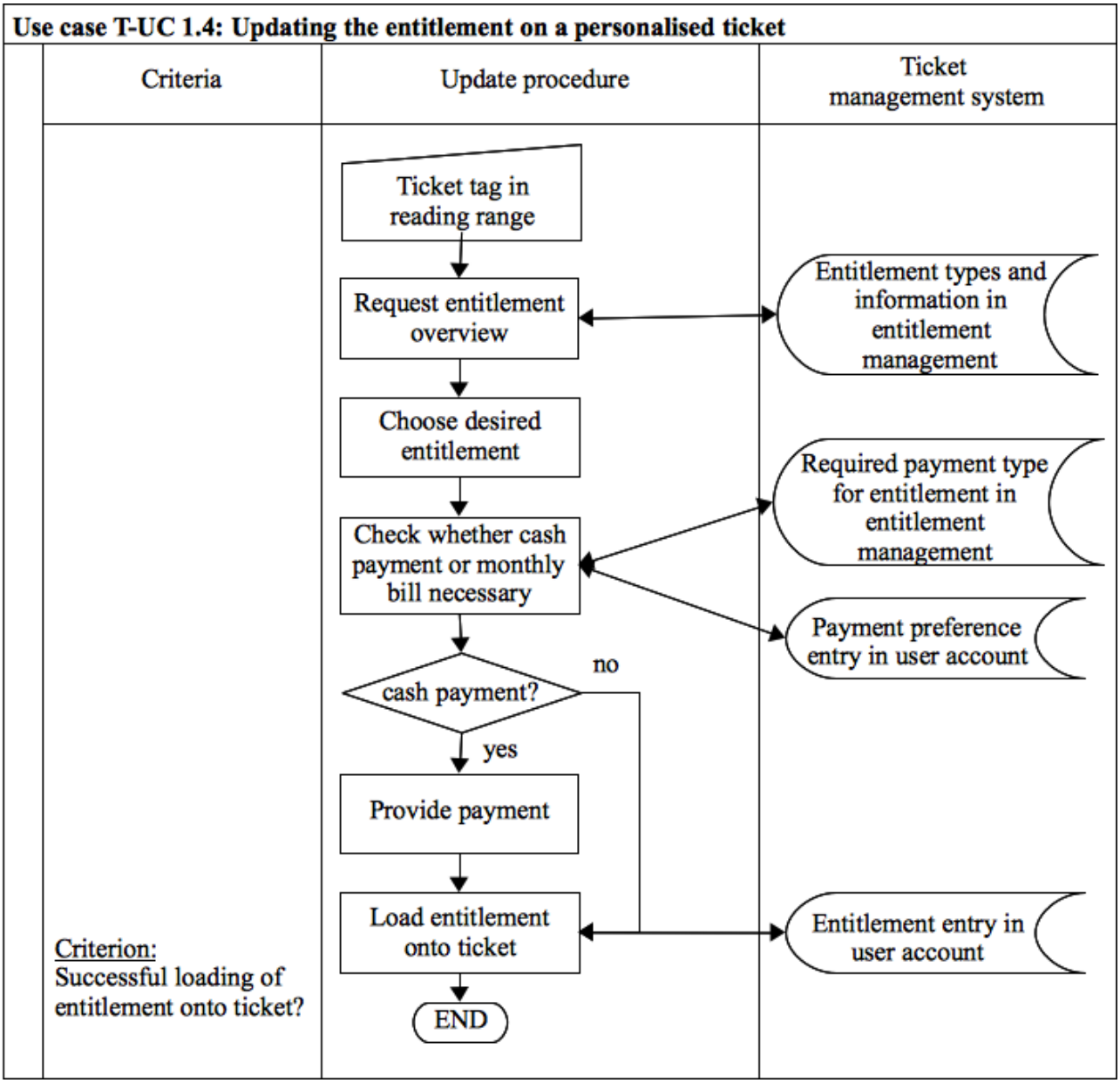

Figure 41: Use case T-UC 1.4 – Updating the entitlement on a personalised ticket

3.2.1.3.5 Use case T-UC 1.5: De-registering from the ticket service

The prerequisite for this use case is the application of a customer for a de-registration. The de-registration request is only accepted and filed for further processing after positively identifying the customer.

When a de-registration request has been filed, the respective data is retrieved from the user account. If there are any card applications registered in the user account, these are blocked and the application-specific black- and whitelists are updated accordingly. In the next step the personalised

ticket itself is blocked and the carrier medium-specific black- and whitelists are updated accordingly. Consequently, the customer cannot use his ticket anymore.

The next step of the de-registration procedure is to add a de-registration entry to the user account. Then it needs to be checked whether the user account has to be deleted. If it does not contain any personal data or references to personal data its data could be saved by the public transport operator and further used for analysis purposes. If the user account contains personal data or the public transport operator does not want to keep the data, the deletion of the user account is scheduled. Now starts a dedicated period of time during which the customer can take back his de-registration request. Only when this period of time elapses, the actual deletion of the user account is performed.

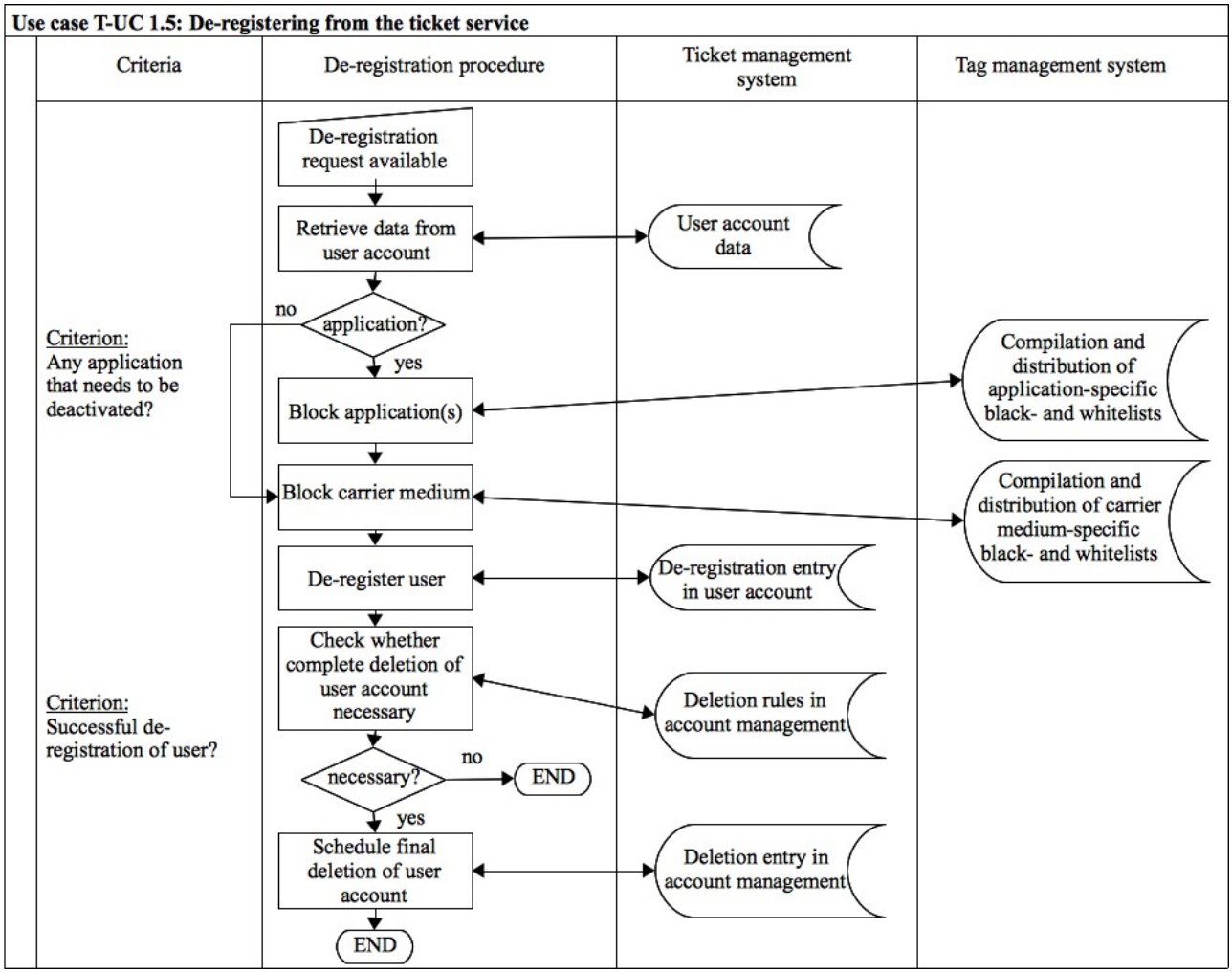

Figure 42: Use case T-UC 1.5 – De-registering from the ticket service

3.2.1.3.6 Use case T-UC 2.1: Registering for a personalised ticket with an existing carrier medium

This use case is identical to T-UC 1.1. The only difference is that during registration the customer needs to inform the public transport operator that he will use a carrier medium that he already owns. So that the procedure to personalise a new ticket card is not initiated.

When the user account is created, the public transport operator will inform the customer that he can now initialise his existing carrier medium either via web application, at a vending machine or at a service point.

3.2.1.3.7 Use case T-UC 2.2: Initialising an existing carrier medium (multi-application card, NFC mobile device)

The existing carrier medium is either initialised with an ID and this ID is then registered in the respective user account or one of its existing IDs is registered in the respective user account. If there is the need for distinct applications, these are initialised and registered in the user account, too.

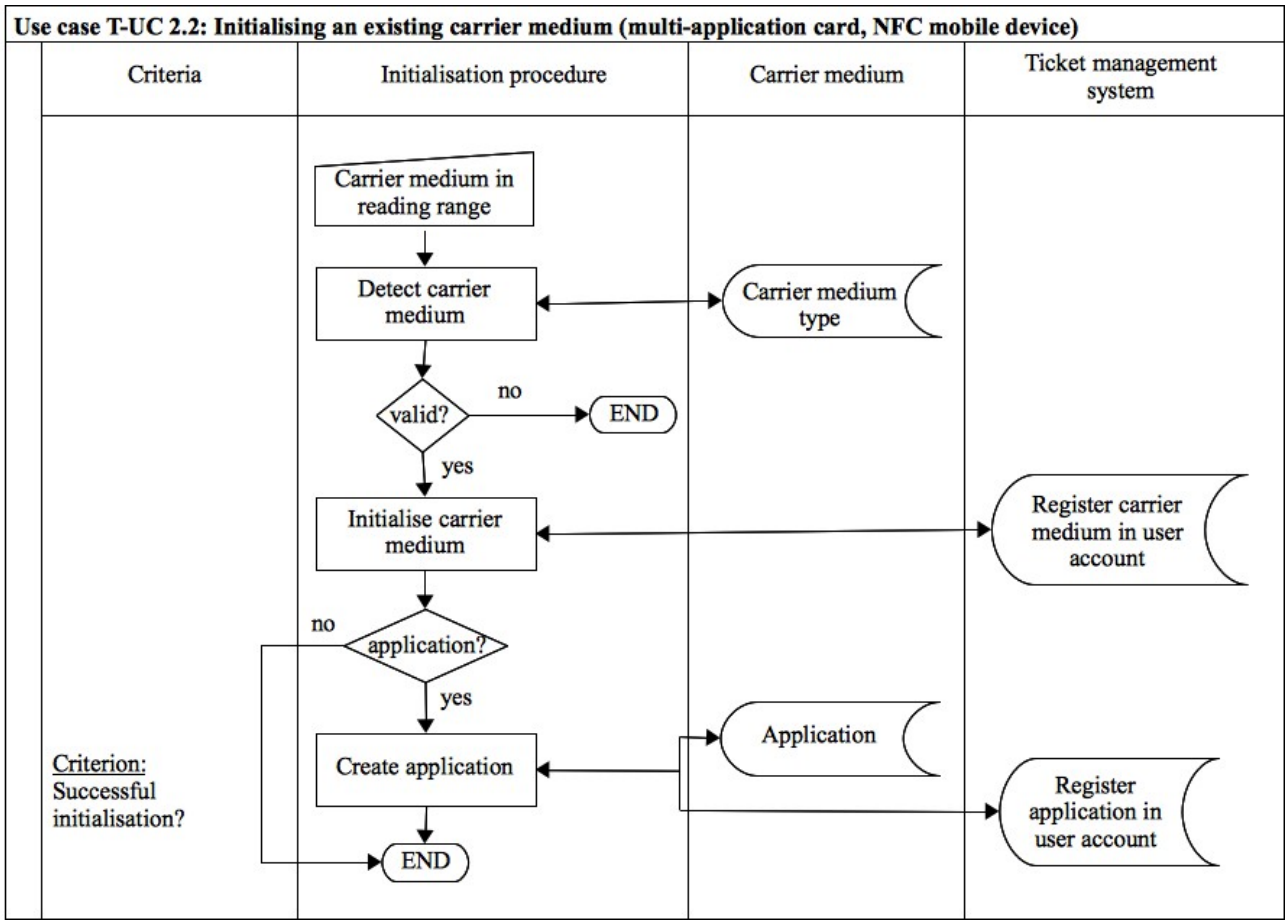

Figure 43: Use case T-UC 2.2 – Initialising an existing carrier medium (multi-application card, NFC mobile device)

3.2.1.3.8 Use case T-UC 2.3: Updating the entitlement with an existing carrier medium

This use case is identical to T-UC 1.4.

3.2.1.3.9 Use case T-UC 2.4: De-registering from the ticket service with an existing carrier medium

This use case is identical to T-UC 1.5.

3.2.1.3.10 Use case T-UC 3.1: Purchasing and loading an entitlement onto a non-personalised ticket

After having fetched a non-personalised ticket, the customer can buy an entitlement and load it onto the ticket. This can either happen via a web application at home or at a vending machine.

The customer first needs to hold his ticket in front of the reader. He is then offered an overview of entitlements that he can purchase. He chooses a specific entitlement and the cash payment transaction is performed. Finally, the entitlement is loaded onto the ticket.

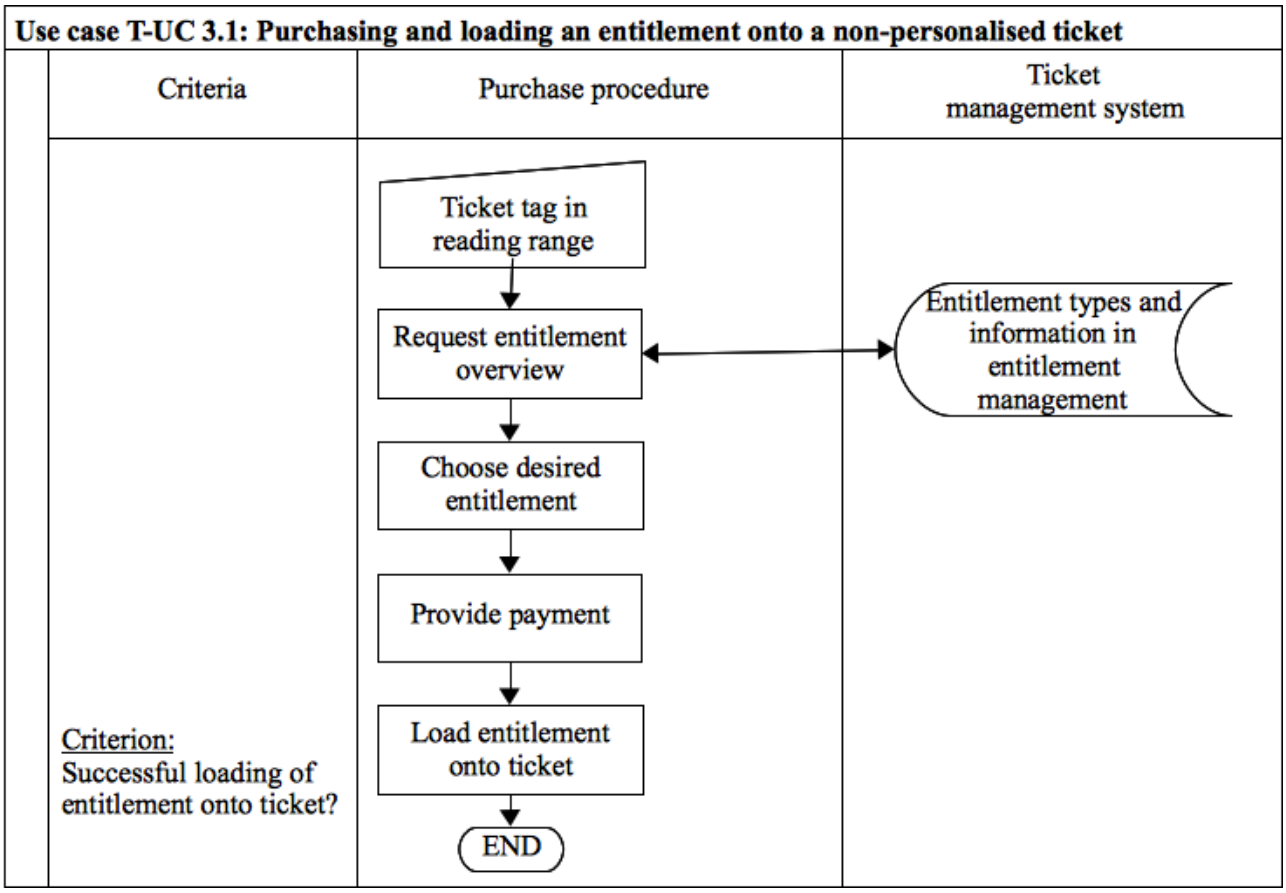

Figure 44: Use case T-UC 3.1 – Purchasing and loading an entitlement onto a non-personalised ticket

3.2.1.3.11 Use case T-UC 4.1a: Checking-in at a gate or when entering a vehicle with a personalised ticket (online case)

When a customer wants to use the public transport, he needs to provide his personalised ticket either at a gate or in the vehicle. Holding his ticket to the reader, a medium and application authentication follows; for a detailed description of this authentication step see figure 7-3 in [BSI2009], page 44. It then

- might be necessary to enter an authentication factor
  In this case, the customer needs to enter e.g. a PIN or a password. Performing such an authentication could guarantee that the ticket is only used by the customer himself.
  This case is not yet in use because it is complex to realize from a procedural point of view.

Nevertheless, it might be feasible in the future and thus, in the following, it is described as an option.

- or not
  In this case, the customer only needs to hold the ticket in front of the reader.

Then the validity of the ticket is checked against the black- and whitelists in the tag management system and the validity of the entitlement is checked as well. If one is not valid, the procedure ends and access to the public transport facility/vehicle is not granted to the customer. If both are valid, the respective user data is retrieved from the user account in the ticket management system and a check-in entry is written to the user account. This check-in entry contains the user's ID, the gate/vehicle ID and a timestamp.

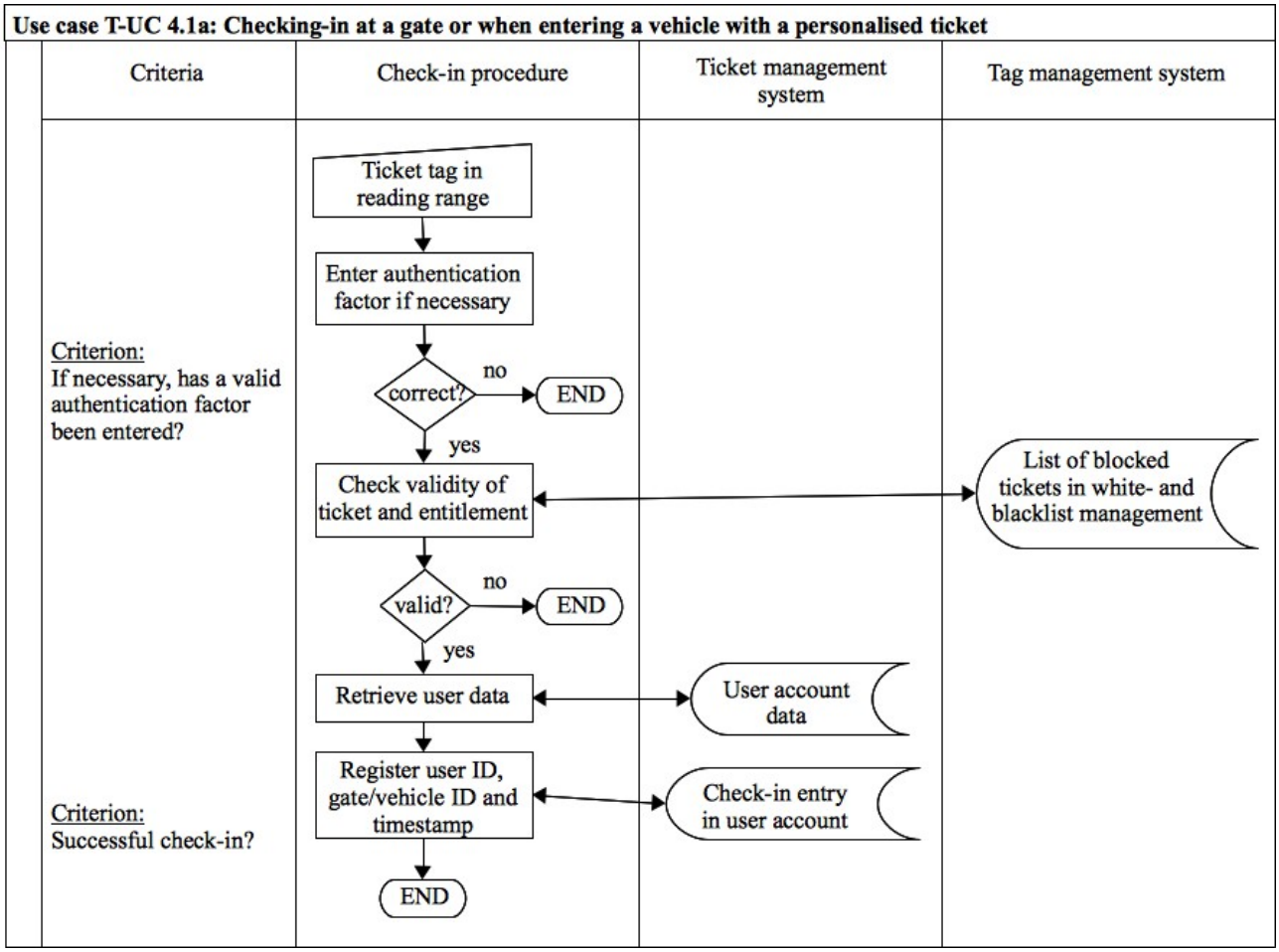

Figure 45: Use case T-UC 4.1a – Checking-in at a gate or when entering a vehicle with a personalised ticket

3.2.1.3.12 Use case T-UC 4.1b: Checking-in at a gate or when entering a vehicle with a non-personalised ticket (online case)

When a customer wants to use the public transport, he needs to provide his non-personalised ticket either at a gate or in the vehicle. Holding his ticket to the reader, a medium and application authentication follows; for a detailed description of this authentication step see figure 7-3 in [BSI2009], page 44. Then the validity of the ticket is checked against the black- and whitelists in the tag management system and the validity of the entitlement is checked as well. If one is not valid,

the procedure ends and access to the public transport facility/vehicle is not granted to the customer. If both are valid, a check-in entry is written to the general usage data base in the ticket management system. This check-in entry contains the ticket's ID, the gate/vehicle ID and a timestamp.

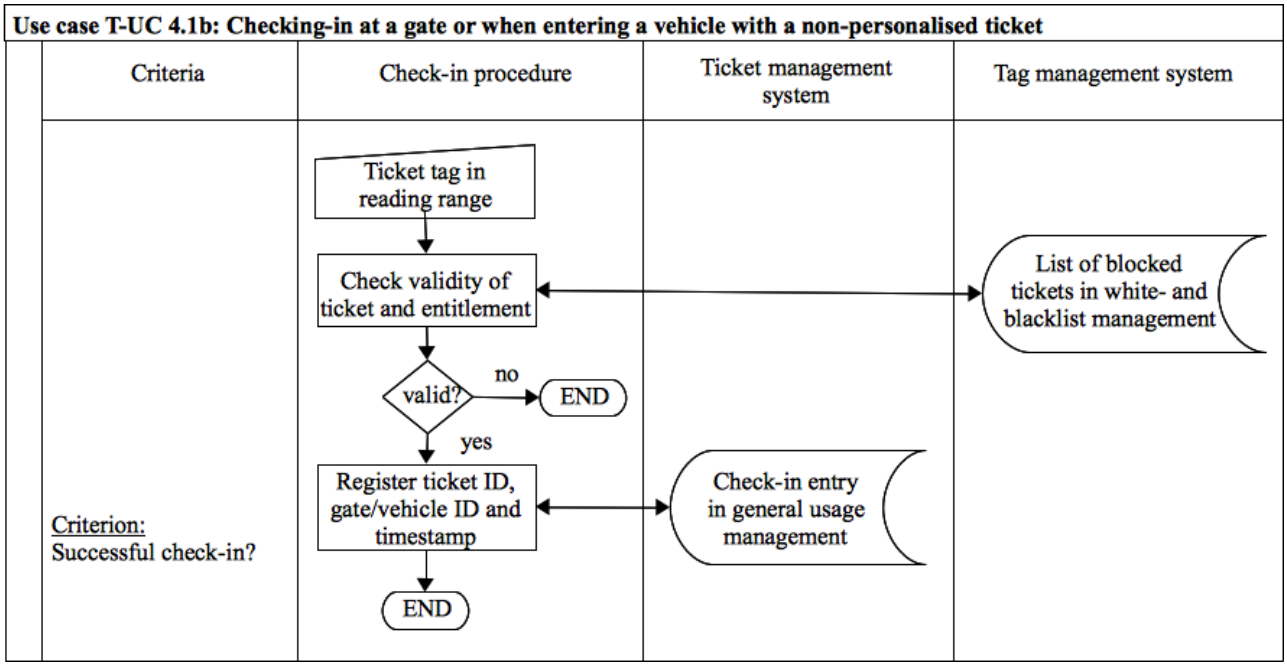

Figure 46: Use case T-UC 4.1b – Checking-in at a gate or when entering a vehicle with a non-personalised ticket

3.2.1.3.13 Use case T-UC 4.1c: Checking-in at a gate or when entering a vehicle with a (non-)personalised ticket (offline case)

In the case, when there is no online connection between the gate/vehicle and the ticket and tag management systems, T-UC 4.1a and 4.1b work differently.

White- and blacklists will be downloaded to the distributed systems of the gates and vehicles at regular time intervals, e.g. once a day. Thus, the validity check is based on the white- and blacklists that are available on the distributed systems at a certain point in time.

The check-in entries are initially stored on the distributed systems of the gates and vehicles and later written to the ticket management system. This might happen at regular time intervals, too, e.g. in the form of batch processes. In this offline case, the user ID of a personalised ticket cannot be retrieved during initial creation of the check-in entries but needs to be derived from the ticket ID during the writing process to the ticket management system.

3.2.1.3.14 Use case T-UC 4.2a: Checking-out when leaving a vehicle or at a gate with a personalised ticket (online case)

When a customer leaves the public transport facilities either through a gate or by leaving a vehicle, he again needs to provide his personalised ticket. A medium and application authentication follows; for a detailed description of this authentication step see figure 7-3 in [BSI2009], page 44.

The respective user data is retrieved from the user account in the ticket management system and a check-out entry is written to the user account. This check-out entry contains the user's ID, the gate/vehicle ID and a timestamp.

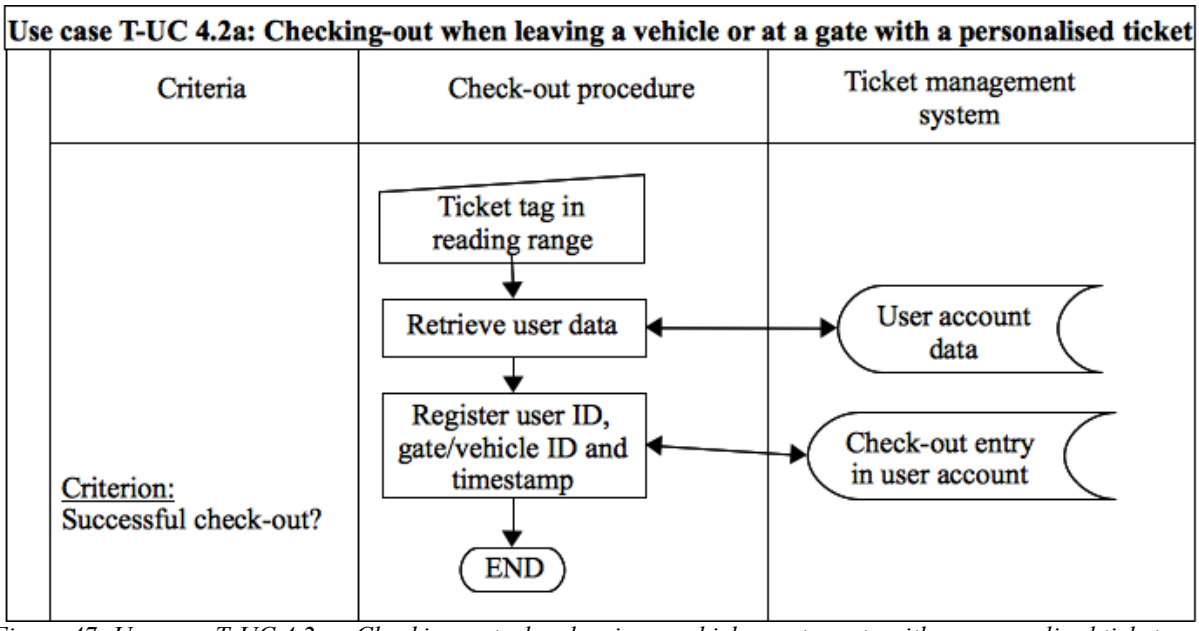

Figure 47: Use case T-UC 4.2a – Checking-out when leaving a vehicle or at a gate with a personalised ticket

3.2.1.3.15 Use case T-UC 4.2b: Checking-out when leaving a vehicle or at a gate with a non-personalised ticket (online case)

When a customer leaves the public transport facilities either through a gate or by leaving a vehicle, he again needs to provide his non-personalised ticket. A medium and application authentication follows; for a detailed description of this authentication step see figure 7-3 in [BSI2009], page 44.

A check-out entry is written to the general usage data base in the ticket management system. This check-out entry contains the ticket's ID, the gate/vehicle ID and a timestamp.

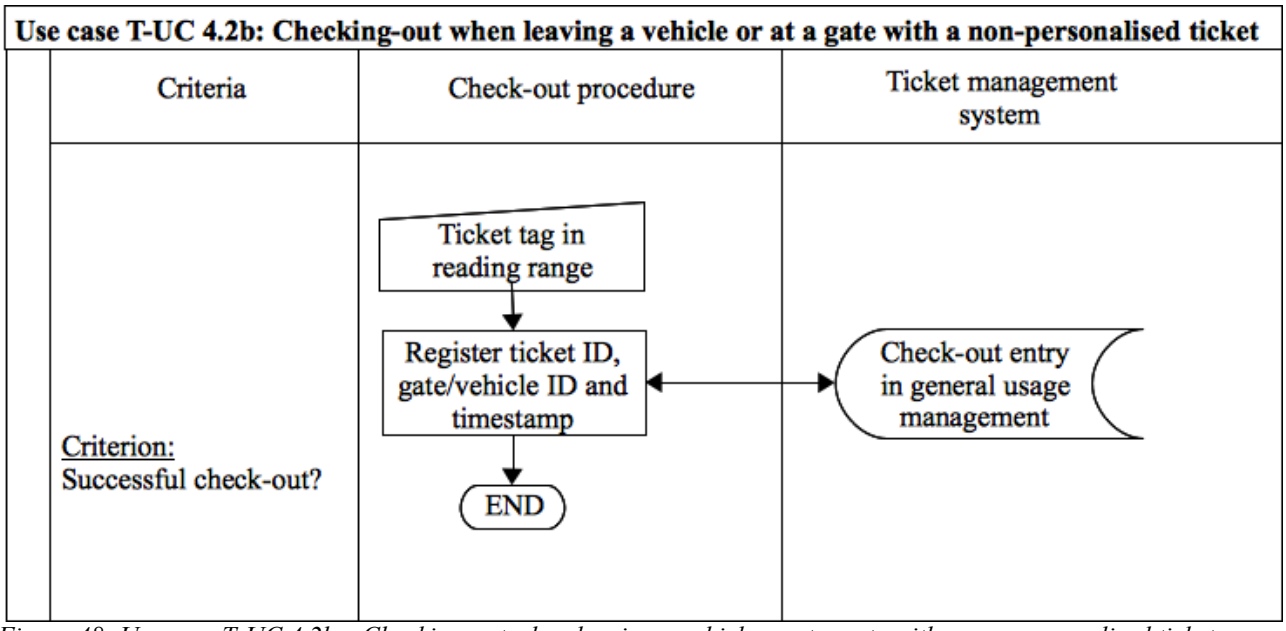

Figure 48: Use case T-UC 4.2b – Checking-out when leaving a vehicle or at a gate with a non-personalised ticket

3.2.1.3.16 Use case T-UC 4.2c: Checking-out when leaving a vehicle or at a gate with a (non-)personalised ticket (offline case)

In the case, when there is no online connection between the gate/vehicle and the ticket management system, T-UC 4.2a and 4.2b work differently.

The check-out entries are initially stored on the distributed systems of the gates and vehicles and later written to the ticket management system. This might happen at regular time intervals, e.g. in the form of batch processes. In this offline case, the user ID of a personalised ticket cannot be retrieved during initial creation of the check-out entries but needs to be derived from the ticket ID during the writing process to the ticket management system.

3.2.1.3.17 Use case T-UC 5.1: Registering for the added-value service

The customer needs to fill out a registration form to register for the added-value service. This can most probably be done via a web application. The application ensures that all necessary personal data has been provided by the customer. In the simplest case, the customer might only provide the identity of his mobile device. If necessary, the customer can prove his identity by providing his eID to the application.

The registration form is then processed and a user account containing the customer's personal data is created in the added-value service management system. Finally, a mobile device entry is written to the user account, which most likely contains the mobile device's identity and thus establishes the link between mobile device and added-value service.

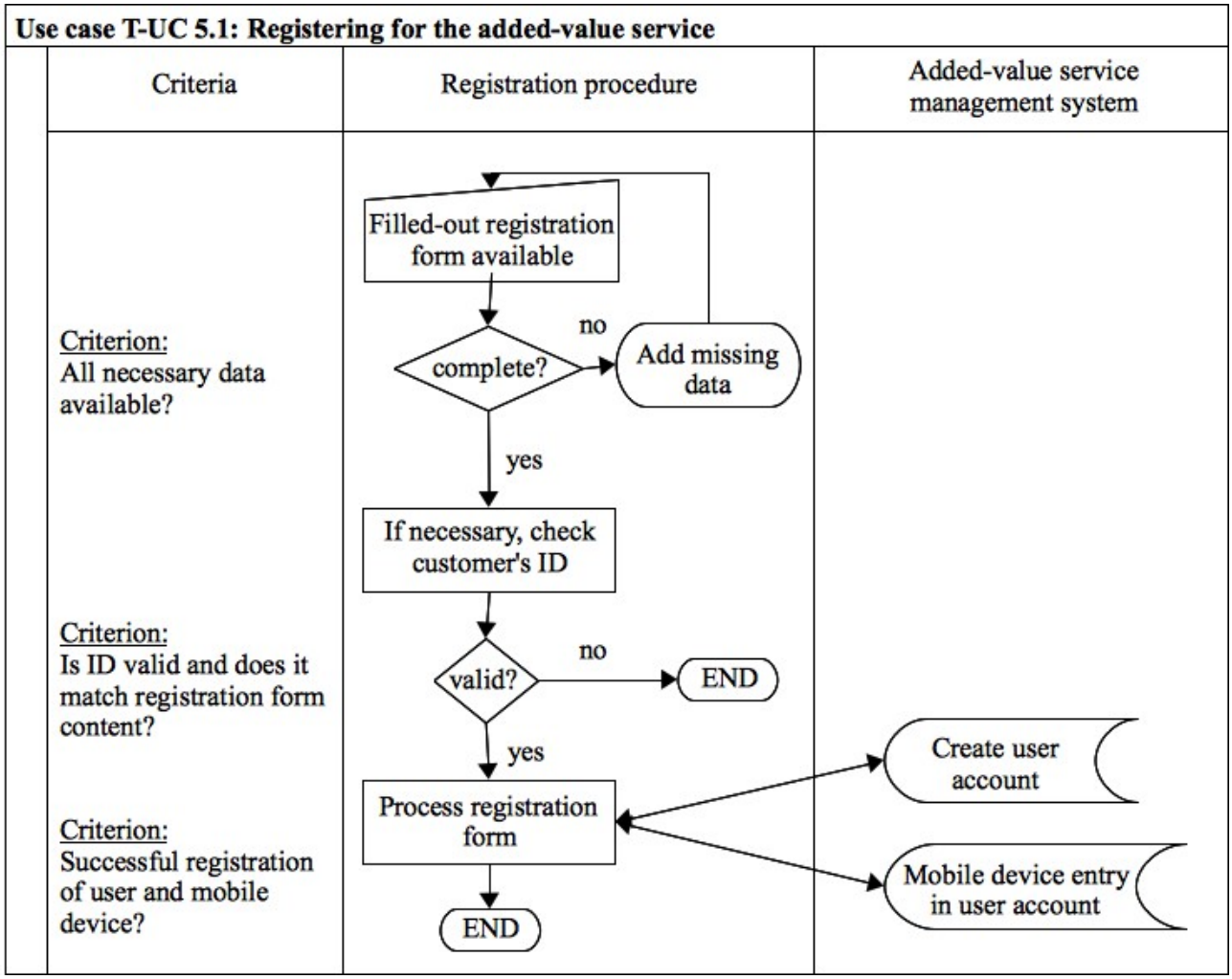

Figure 49: Use case T-UC 5.1 – Registering for the added-value service

3.2.1.3.18 Use case T-UC 5.2: Getting personalised information from the added-value service

The added-value service offers pull and push services. If the customer requests one of the offered services either by having configured his account (push) or by requesting a service at a specific moment in time via his mobile device (pull), the respective user data is retrieved from the user account in the added-value service management system.

Then, if necessary and with the customer's consent, the mobile device is localised. The computed locality is then registered in the user's account together with a timestamp. This locality is then combined with service and preference entries in the user account to be able to personalise and adapt the requested service accordingly. Before providing the requested service, it is checked whether this service is available under the current conditions (locality, preferences, technical availability). If it is not available, the procedure is aborted and an error message is displayed. If the service is available, the respective service information is provided.

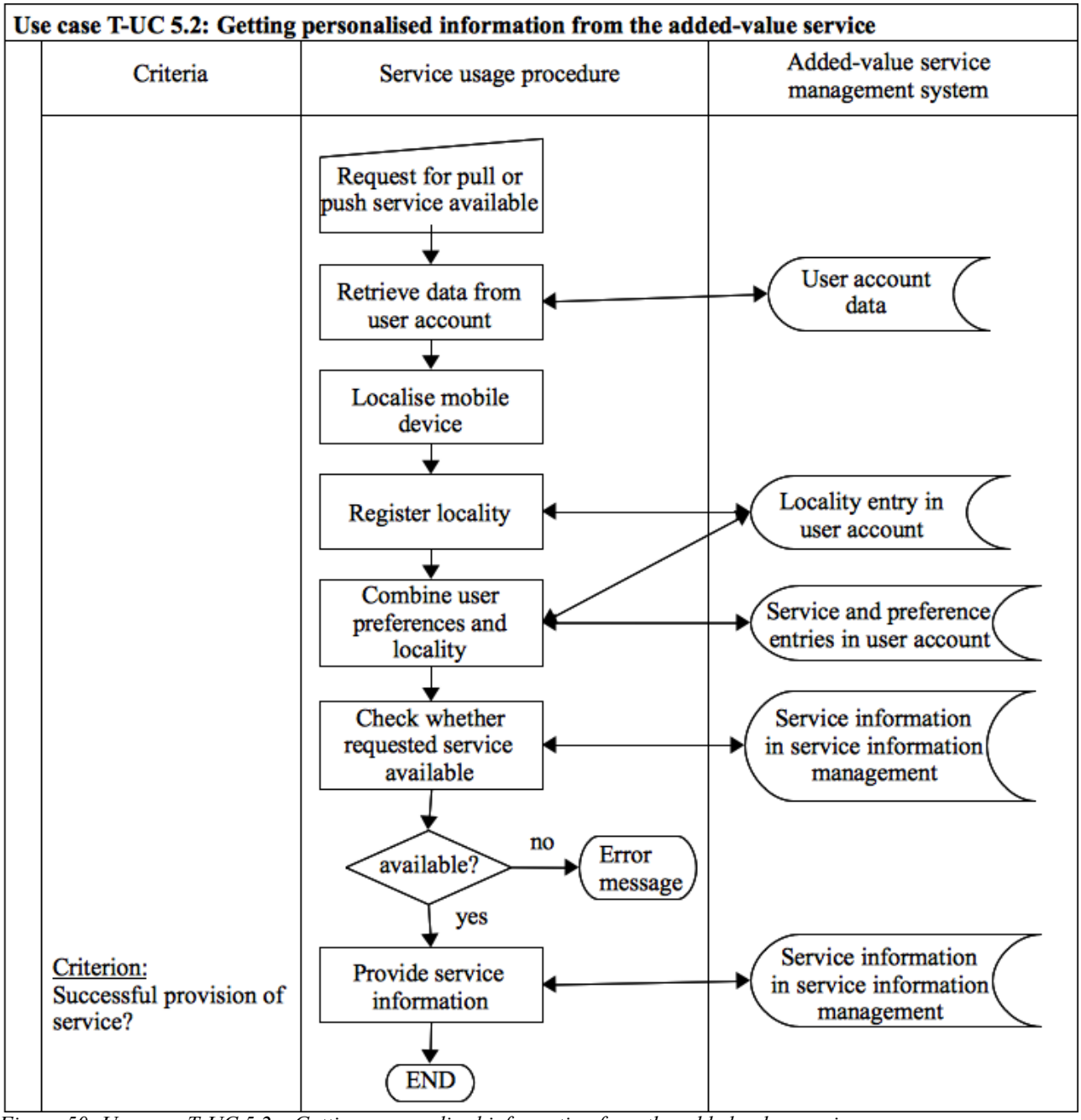

Figure 50: Use case T-UC 5.2 – Getting personalised information from the added-value service

3.2.1.3.19 Use case T-UC 5.3: De-registering from the added-value service

The prerequisite for this use case is the application of a customer for a de-registration. The de-registration request is only accepted and filed for further processing after positively identifying the customer.

When a de-registration request has been filed, the respective data is retrieved from the user account. The user account is then blocked and the account-specific black- and whitelists are updated accordingly. Consequently, the customer cannot use his user account anymore.

The next step of the de-registration procedure is to add a de-registration entry to the user account. It then needs to be checked whether the user account has to be deleted. If it does not contain any personal data or references to personal data its data could be saved by the added-value service provider and further used for analysis purposes. If the user account contains personal data or the added-value service provider does not want to keep the data, the deletion of the user account is scheduled. Now starts a dedicated period of time during which the customer can take back his de-registration request. Only when this period of time elapses, the actual deletion of the user account is performed.

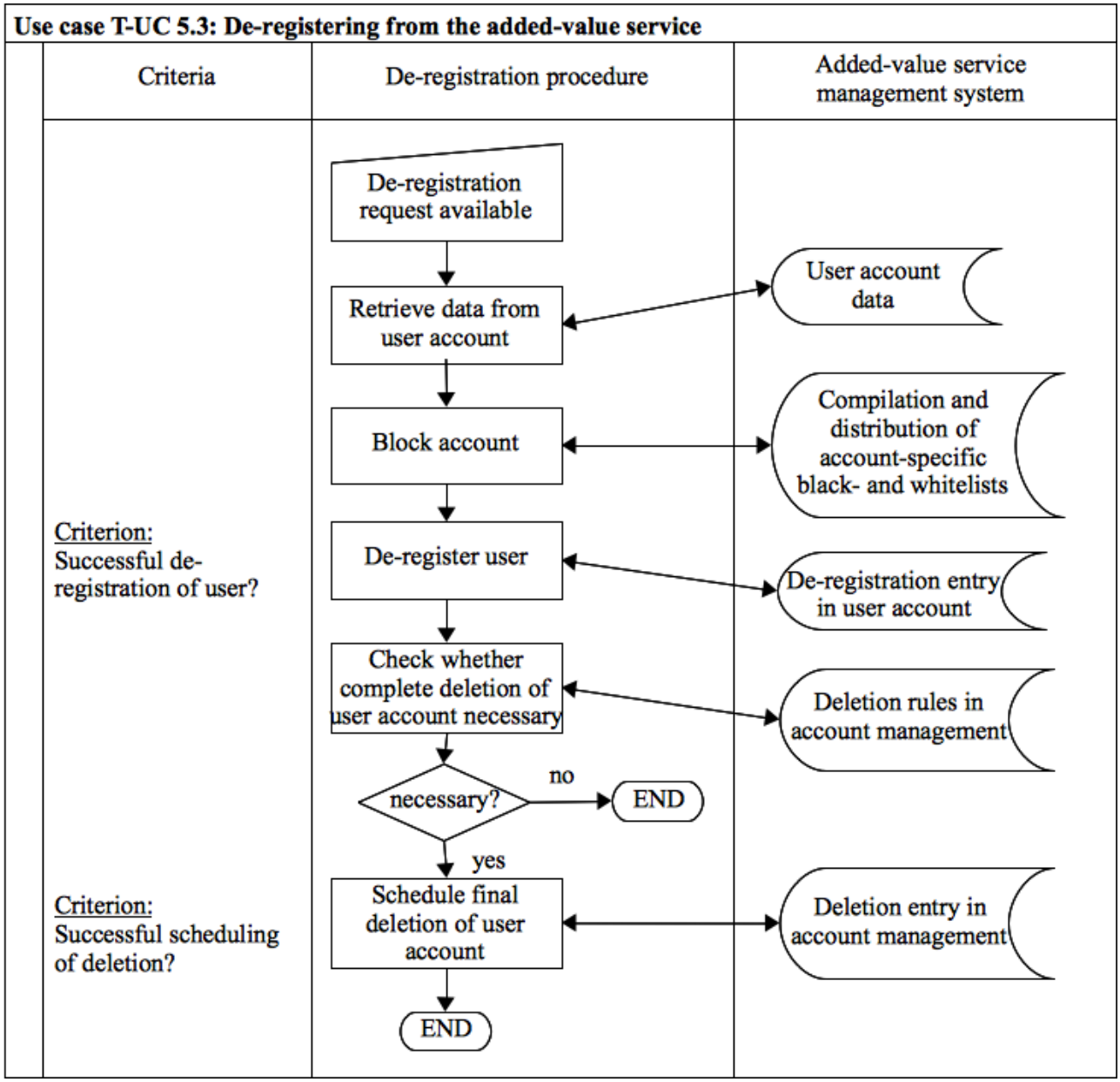

Figure 51: Use case T-UC 5.3 – De-registering from the added-value service

3.2.2 Step 2: Definition of privacy targets

In this step, stakeholders should discuss the privacy targets that are described in the PIA Framework and the concrete instances of those privacy targets as described in the PIA guideline. By discussing the targets and their instances, stakeholders can clarify what the targets mean in the context of the specific RFID application and corresponding business cases.

Privacy target code and name		**Contextual explanation**	**Examples for how to reach this target**
P1.1	Ensuring fair and lawful	The operator must explain the RFID technology that is used in the personalised and non-personalised tickets	Use the RFID-emblem, informational material, flyers, web

Privacy target code and name		Contextual explanation	Examples for how to reach this target
	processing through transparency	as well as the workings of the readers in the gates and vehicles to the customers in a way that helps them understand the benefits and consequences. Customers should understand that they can choose between personalised and non-personalised tickets.	pages, and training for customer support personnel.
P1.2	Providing purpose specification and limitation	The operator must specify the purpose for which customer data is collected when receiving and using personalised and non-personalised tickets. It should be clear for which purposes the data is used and whether it is handed over to third parties.	Write clear internal and external purpose specifications so that access rights can be handled accordingly and customers are well informed about what their personal data is used for.
P1.3	Ensuring data avoidance and minimisation	When designing and implementing the ticket, transport and added-value service management systems, the operator should ensure that only necessary customer data is collected and processed. In this context, necessary means that the information is necessary for the fulfilment of the specified purpose.	Ensure that customers can choose between personalised (T-P1, T-P2) and non-personalised tickets (T-P3). Collect only the customer data that is needed to offer the services of monthly billing and best price models.
P1.4	Ensuring quality of data	The operator must check the customer data that is stored in the user account management of the ticket and added-value management system to ensure that it is correct and up-to-date. Monthly billing, best price models and the provision of travel-related information heavily depend on correct customer data.	Check registration forms thoroughly (T-P1.1, T-P2.1, T-P5.1). Regularly remind customers to check that their user accounts are correct and up-to-date.
P1.5	Ensuring limited duration of data storage	Customer data should only be stored and processed as long as it is needed for the specified purpose.	Implement strict erasure rules that are executed when customers de-register (T-P1.5, T-P2.4, T-P5.3). If possible, regularly erase some of the customer data after a specified period of time.
P2.1	Legitimacy of processing personal data	When customers register for the acquisition of personalised tickets and the added-value service, the validity of their consent should be thoroughly checked.	Check registration forms and identification thoroughly (T-P1.1, T-P2.1, T-P5.1).
P3.1	Legitimacy of processing sensitive personal data	- not applicable in this scenario - No sensitive personal data is collected or processed in this scenario.	- not applicable in this scenario -
P4.1	Providing adequate information in cases of direct collection of data from the data subject	As data is directly collected from the customers through the acquisition and usage of tickets, the provision of information that describes the collected data should be ensured.	Provide adequate information, see P1.1.

Privacy target code and name		Contextual explanation	Examples for how to reach this target
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	- not applicable in this scenario - No data that is directly obtained from the customer, e.g. data from third parties, is processed in this scenario.	- not applicable in this scenario -
P5.1	Facilitating the provision of information about processed data and purpose	Customers must be provided with information about the purpose of the data collection and about the collected data categories.	Provide adequate information, see P1.1.
P5.2	Facilitating the rectification, erasure or blocking of data	Customers should be allowed to rectify, erase or block their data. User accounts in both the ticket and added-value service management systems need to be considered.	Enable customers to rectify, erase or block data about themselves via a web application. Provide customers with a contact address, form or the like that they can use to request rectification, erasure or blocking of their data.
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	- not applicable in this scenario - No consumer data is handed over to a third party in this scenario, thus there is no need to consider this privacy target.	- not applicable in this scenario -
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	- not applicable in this scenario - Customers must be able to object to the processing of their data for direct marketing purposes or disclosure to third parties. No customer data is disclosed to third parties in this scenario. Customer data is not used for the purpose of direct marketing in this scenario.	- not applicable in this scenario -
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	- not applicable in this scenario - Customers must be able to object to being subject to automated decisions. No automated decisions are used in this scenario.	- not applicable in this scenario -
P7.1	Safeguarding confidentiality and security of processing	BSI's TG 03126-1 needs to be considered.	---

Privacy target code and name		Contextual explanation	Examples for how to reach this target
P8.1	Compliance with notification requirements	Before going live with the selling and management of personalised and non-personalised tickets as well as the added-value service, the supervisory data protection authority needs to be notified about the related processing of personal data. The operator must provide the results of the PIA to the supervisory authority six weeks before the launch.	The public transport service provider and the added-value service provider should assign a person in their organisation to take care of these notifications. The assignee might need a project team to create the necessary documentation.

Table 28: Public transport PIA – Definition of privacy targets

3.2.3 Step 3: Evaluation of protection demand categories

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.1	Ensuring fair and lawful processing through transparency	1	1	2	2	2	2

If the data processing activities related to the system landscape are not made transparent internally as well as externally to customers or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because most of the customers should easily understand the workings of the service as it is not so different from ticket systems that are already in use elsewhere. Customers might already be familiar with it.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired and thus there is no need for costly image campaigns or adaptations to the ticket system.
- customers' reputation can be seriously adversely affected if their movement profiles reveal sensitive personal information about their lifestyle (i.e. visits to doctors, unusual movement within working hours, etc.).
- customers' financial well-being can be seriously adversely affected if their movement profiles reveal sensitive personal information about their lifestyle (i.e. visits to doctors shared with insurance companies, unusual movement within working hours shared with employees, etc.).
- customers' personal freedom could be endangered if they decided to participate in a personalized ticket system without full knowledge of the tracing activities taking place.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 29: Public transport PIA – Definition of protection demand categories for P1.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.2	Providing purpose specification and limitation	3	2	2	2	2	3

If the purpose and limitations of data processing are not specified, the RFID operator risks engaging in processing that is beyond the purposes for which data has been initially collected from data subjects. If such processing becomes known to the public, customers, journalists or the authorities, the parties that are involved may face the following consequences:

- the operator's reputation can suffer nation-wide impairment if detailed data about customers' public transport usage is used for purposes that were not specified, and the data is accessed by unauthorised parties, customers might be considerably impaired.
- the operator's financial loss can be considerable if its reputation is heavily impaired and the resulting costly actions need to be undertaken.
- customers' reputation can be seriously adversely affected if their detailed data about public transport usage becomes known to unauthorised parties and is used for purposes that were not specified and agreed upon. For example, the data might be used to analyse their lifestyle (i.e. visits to doctors, unusual movement within working hours, etc.).
- customers' financial well-being can be seriously adversely affected if their movement profiles reveal sensitive personal information about their lifestyle (i.e. visits to doctors shared with insurance companies, unusual movement within working hours shared with employees, individual prices being adapted).
- customers' personal freedom could be endangered if their detailed data about public transport usage becomes known to unauthorised parties who abuse this knowledge.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 30: Public transport PIA – Definition of protection demand categories for P1.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.3	Ensuring data avoidance and minimisation	1	1	2	2	1	2

The operator wants to minimise customers' privacy concerns as well as information and notification duties that depend on the amount of personal data processed. More data also implies a need for the often costly implementation of sophisticated technical controls to secure the collected personal data.

If the principles of data avoidance and minimisation are not realised throughout the relevant applications and services, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because it is not very likely that customers will find out that the operator collects more data than necessary if the operator sticks to the specified purpose and services.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there should be no need for costly image campaigns or adaptations (especially the implementation of data minimisation measures) of the ticket system.
- customers' reputation can be seriously adversely affected if more and/or more detailed data is collected than is necessary for the specified purpose and services. For example, the data might be used to analyse their lifestyle (i.e. visits to doctors, unusual movement within working hours, etc.).
- customers' financial well-being can be seriously adversely affected if more and/or more detailed data is collected than is necessary for the specified purpose and services (i.e. visits to doctors shared with insurance companies, unusual movement within working hours shared with employees, individual prices being adapted).
- customers' personal freedom cannot be endangered.

As two of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 31: Public transport PIA – Definition of protection demand categories for P1.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.4	Ensuring quality of data	2	2	1	2	1	2

If the quality (accuracy, up-to-dateness, or completeness) of the personal data that is collected and processed is not ensured, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because customers might object to wrongly computed bills and might be dissatisfied by inappropriate information from the added-value service.
- the operator's financial loss can be considerable if its reputation is considerably impaired and thus leads to costly corrections of the ticketing system and costly image campaigns to restore customers' faith.
- customers' reputation can be adversely affected if they get wrongly computed bills and/or are misinformed and thus cannot travel optimally, resulting in lateness or other negative outcomes.
- customers' financial well-being can be seriously adversely affected if they get wrongly computed bills and thus have to pay more.
- customers' personal freedom cannot be endangered.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 32: Public transport PIA – Definition of protection demand categories for P1.4

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.5	Ensuring limited duration of data storage	1	1	2	2	1	2

If data is stored longer than necessary and no clear rules are implemented to limit data storage, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because it is not very likely that customers will find out that the operator stores data longer than necessary if the operator sticks to the specified purpose and services.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there should be no need for costly image campaigns or adaptations (especially the implementation of erasure measures) of the ticket system.
- customers' reputation can be seriously adversely affected if detailed data is stored longer than is necessary for the specified purpose and services. If data accumulates, the operator might be able to trace the customers' locations for a long period of time. For example, the data might be used to analyse the customers' lifestyle (i.e. visits to doctors, unusual movement within working hours, etc.).
- customers' financial well-being can be seriously adversely affected if detailed data is stored longer than is necessary for the specified purpose and services. If data accumulates, the operator might be able to trace the customers' locations for a long period of time (i.e. visits to doctors shared with insurance companies, unusual movement within working hours shared with employees, individual prices being adapted).
- customers' personal freedom cannot be endangered.

As two of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 33: Public transport PIA – Definition of protection demand categories for P1.5

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P2.1	Legitimacy of processing personal data	3	2	2	2	1	3
If the legitimacy of processing personal data is not ensured, e.g. via consent, the parties that are involved may face the following consequences: - the operator's reputation can suffer nation-wide impairment because customers, especially those using personalised tickets, might feel betrayed and initiate lawsuits. - the operator's financial loss can be considerable reputation is heavily impaired and results in costly image campaigns, adaptations of the ticket system and costs for potential lawsuits. - customers' reputation can be seriously adversely affected if detailed personal data (i.e. visits to doctors, unusual movement within working hours, etc.) is collected, stored and processed that they are not aware of. - customers' financial well-being can be seriously adversely affected if detailed personal data (i.e. visits to doctors, unusual movement within working hours, etc.) is collected, stored and processed that they are not aware of. - customers' personal freedom cannot be endangered. As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.							

Table 34: Public transport PIA – Definition of protection demand categories for P2.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P3.1	Legitimacy of processing sensitive personal data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 35: Public transport PIA – Definition of protection demand categories for P3.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.1	Providing adequate information in cases of direct collection of data from the data subject	1	1	2	2	2	2

This privacy target is strongly related to P1.1, thus a similar analysis is used.

If the data processing activities related to the system landscape are not made transparent internally as well as externally to customers or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because most of the customers should easily understand the workings of the service as it is not so different from ticket systems that are already in use elsewhere. Customers might already be familiar with it.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired and thus there is no need for costly image campaigns or adaptations to the ticket system.
- customers' reputation can be seriously adversely affected if their movement profiles reveal sensitive personal information about their lifestyle (i.e. visits to doctors, unusual movement within working hours, etc.).
- customers' financial well-being can be seriously adversely affected if their movement profiles reveal sensitive personal information about their lifestyle (i.e. visits to doctors shared with insurance companies, unusual movement within working hours shared with employees, etc.).
- customers' personal freedom could be endangered if they decided to participate in a personalized ticket system without full knowledge of the tracing activities taking place.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 36: Public transport PIA – Definition of protection demand categories for P4.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 37: Public transport PIA – Definition of protection demand categories for P4.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.1	Facilitating the provision of information about processed data and purpose	1	1	1	1	1	1
If no information about processed data (i.e. in the form of data categories and items) and purpose is provided to the customers, the parties that are involved may face the following consequences: - the operator's reputation can be minimally impaired because only a few customers might enforce their legal rights and force the operator to provide a detailed overview of their processed data. - the operator's financial loss can be acceptable because generating detailed data processing reports for some customers might not be too costly. - customers' reputation cannot be affected significantly. - customers' financial well-being cannot be affected significantly. - customers' personal freedom cannot be endangered. As all of the criteria are evaluated as being low, the overall evaluation is “low – 1”.							

Table 38: Public transport PIA – Definition of protection demand categories for P5.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.2	Facilitating the rectification, erasure or blocking of data	2	2	1	2	1	2
This privacy target is strongly related to P1.4, thus a similar analysis is used. If customers are not enabled to rectify, erase or block their personal data, the parties that are involved may face the following consequences: - the operator's reputation can be considerably impaired because customers might object to wrongly computed bills (because of incorrect data). Customers might also be dissatisfied by information from the added-value service that is not personally appropriate. - the operator's financial loss can be considerable if its reputation is considerably impaired. Such damage can result in costly corrections of the ticketing system and costly image campaigns to restore customers' faith. - customers' reputation cannot be affected significantly. - customers' financial well-being can be seriously adversely affected if they get wrongly computed bills and thus have to pay more. - customers' personal freedom cannot be endangered. As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.							

Table 39: Public transport PIA – Definition of protection demand categories for P5.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 40: Public transport PIA – Definition of protection demand categories for P5.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 41: Public transport PIA – Definition of protection demand categories for P6.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 42: Public transport PIA – Definition of protection demand categories for P6.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P7.1	Safeguarding confidentiality and security of processing	-	-	-	-	-	---
BSI's TG 03126-1 needs to be considered.							

Table 43: Public transport PIA – Definition of protection demand categories for P7.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P8.1	Compliance with notification requirements	2	2	-	-	-	2
If the operator does not comply with the legally specified notification requirements, the operator may face the following consequences: - the operator's reputation can be considerably impaired because he might get into conflict with the supervisory data protection authority. These conflicts might be exposed to the public. - the operator's financial loss can be considerable if he is forced to pay fines, create the necessary documentation ad-hoc with the help of costly consultants and be subject to regular controls by the supervisory authority in the future. As all of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.							

Table 44: Public transport PIA – Definition of protection demand categories for P8.1

3.2.4 Step 4: Identification of relevant threats

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			operator.		
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	y	
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	y	
		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.	y	
		T1.5	Existing information describing the service is not kept up-to-date.	y	
		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.	y	
	Lack of transparency – Missing or insufficient privacy statement	T1.7	No privacy statement is available.	y	
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	y	
		T1.9	The existing privacy statement does not provide a contact information to reach the RFID Operator and does not provide contact details in case of questions or complaint.	y	
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	y	
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	n	Customer data is not handed over to third parties.
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	y	
	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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			collection process.		
		T1.14	No RFID emblem is displayed on the product and the product packaging.	y	Tickets are the only "objects" that contain RFID tags.
	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.	y	
		T1.16	The data collection purpose is not documented in an adequate way.	y	
		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.	y	
	Collection and/or combination of data exceeding purpose	T1.18	Collected data is processed for other purposes than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	y	This threat is related to TS10 "Unjustified gathering and storing of data" ([BSI2009], p. 67).
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	y	
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	y	This threat is related to TS10 "Unjustified gathering and storing of data" ([BSI2009], p. 67).
		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.	y	This threat is related to TS10 "Unjustified gathering and storing of data" ([BSI2009], p. 67).
		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.	y	
		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	y	This threat is related to TM11 "Tracking by means of unauthorised scanning by third parties"

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			protection.		([BSI2009], p. 64).
	Missing quality assurance of data	T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	y	
		T1.25	The identification of the data subject is not conducted thoroughly.	y	
		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.	y	
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	y	
	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	y	This threat is related to TS10 “Unjustified gathering and storing of data” ([BSI2009], p. 67).
		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.	y	
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.	y	
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	y	
		T2.3	The relevant legal basis (e.g. consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.	y	
T3	Invalidation or non-existence of explicit consent	T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		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.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
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: - 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.	y	
		T4.2	The relevant information is not provided in an adequate form (e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	y	
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	y	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: - 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.	n	This threat belongs to P4.2, which was excluded from further consideration in step 2.
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	n	This threat belongs to P4.2, which was excluded from further consideration in

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
					step 2.
		T4.6	The relevant information is not easily understandable so that it is possible that the data subject will not be able to understand that the operator obtained information on him or her from a third party.	n	This threat belongs to P4.2, which was excluded from further consideration in step 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.	y	
		T5.2	Access is possible but not to all relevant data, including: - 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.	y	
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	y	
		T5.4	Successful access as well as subsequent data disclosure is not logged.	y	
	Inability to rectify, erase or block individual data	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.	y	
		T5.6	Errors are not automatically rectified.	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		T5.7	There is no procedure that allows the erasure of individual data in back-up data.	y	
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	y	
		T5.9	Successful rectification, erasure and blocking is not logged.	y	
	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.	n	This threat belongs to P5.3, which was excluded from further consideration in step 2.
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.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
		T6.3	The operator has not implemented any procedure that would allow the notification of relevant third parties in the case that a data subject has objected to the processing of his personal data.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
	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.	n	This threat belongs to P6.2, which was excluded from further consideration in step 2.
T7	Refer to security-relevant threats that are defined in BSI's technical guidelines TG 03126-4.	T7.1	Refer to the description of security-relevant threats that are defined in BSI's technical guidelines TG 03126-1.	y	BSI's TG 03126-1 needs to be considered.
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.	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		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.	y	
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	y	
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	y	

Table 45: Public transport PIA – Identification of relevant threats

3.2.5 Step 5: Identification and recommendation of controls

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.1	C1.1 C1.4	SERVICE DESCRIPTION INFORMATION TIMELINESS	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.2	C1.2	INFORMATION ACCESSIBILITY	2 (P1.1)	The information describing the service is made accessible at the operator's physical facilities and online.
T1.3	C1.1	SERVICE DESCRIPTION	3 (max of P1.1 and P1.2)	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.
T1.4	C1.1 C1.3	SERVICE DESCRIPTION LANGUAGE / SEMANTICS OF INFORMATION	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. 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). The information describing the service is available in the most

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				common languages and in languages that are potentially specific to its target countries.
T1.5	C1.4	INFORMATION TIMELINESS	2 (P1.1)	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.6	C1.1	SERVICE DESCRIPTION	3 (max of P1.1 and P1.2)	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	INFORMATION ACCESSIBILITY		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.
T1.7	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.8	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.9	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.10	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.12	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.13	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.14	C1.6	RFID EMBLEM	2	The RFID emblem is shown in such a way that it is clearly

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
			(P1.1)	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.
T1.15	C1.7	PURPOSE SPECIFICATION	3 (P1.2)	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.
T1.16	C1.7	PURPOSE SPECIFICATION	3 (max of P1.1 and P1.2)	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.
T1.17	C1.8	ENSURING LIMITED DATA PROCESSING	3 (P1.2)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level.
T1.18	C1.8 C1.9	ENSURING LIMITED DATA PROCESSING ENSURING PURPOSE RELATED PROCESSING	3 (max of P1.3 and TS10 ([BSI2009], p. 111, 124))	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. 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. Related safeguard from [BSI2009]: **MS17** “Satisfying the data minimization obligation”: “Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
T1.19	C1.9	ENSURING PURPOSE RELATED PROCESSING	2 (P1.3)	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.
T1.20	C1.10	ENSURING DATA MINIMISATION	3 (max of P1.3 and TS10 ([BSI2009], p. 111, 124))	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
T1.21	C1.10	ENSURING DATA MINIMISATION	3 (max of P1.3 and TS10 ([BSI2009], p. 111,	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. Additionally, there are technical procedures in place, which

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
			124))	ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
T1.22	C1.8	ENSURING LIMITED DATA PROCESSING	2 (P1.3)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.
T1.23	C1.11	ENSURING TAG PROTECTION	2 (max of P1.3 and TM11 ([BSI2009], p. 138, 149, 161))	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguard from [BSI2009]: **MM8** "Introduce proximity technology as defined by ISO/IEC14443": "Introduce proximity technology as defined by ISO/IEC14443." (p. 83)
T1.24	C1.12	ENSURING PERSONAL DATA QUALITY	2 (P1.4)	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.
T1.25	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2 (P1.4)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.26	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	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.
T1.27	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	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.
T1.28	C1.15	ENABLING DATA DELETION	3 (max of P1.5 and TS10 ([BSI2009], p. 111, 124))	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. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
T1.29	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T2.1	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				employees are taught about this subject during regular privacy training sessions to increase their awareness.
T2.2	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.3	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T4.1	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.2	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T4.3	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T5.1	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T5.2	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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.
T5.3	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	1 (P5.1)	The data subject needs to identify or authenticate him or herself with his or her name and some security questions.
T5.4	C5.2	LOGGING ACCESS TO PERSONAL DATA	1 (P5.1)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T5.5	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.6	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				describe involved roles / employees, required actions and a time frame for answering a data 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.
T5.7	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.8	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2 (P5.2)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
T5.9	C5.2	LOGGING ACCESS TO PERSONAL DATA	2 (P5.2)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T7.1	C7.1	SECURITY CONTROLS	--- (P7.1)	See relevant controls from TG 03126-1.
T8.1	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application’s launch.
T8.2	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application’s launch.
T8.3	C8.2	PRIOR CHECKING	2 (P8.1)	It is ensured that the legally required checking of the RFID application is executed by expert personnel.
T8.4	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				available to the authorities at least 6 weeks prior to the RFID application's launch.

Table 46: Public transport PIA – Identification and recommendation of controls

3.2.5.1 Consolidated view of identified controls

Control code and name		Highest overall category	Description
C1.1	SERVICE DESCRIPTION	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	INFORMATION ACCESSIBILITY	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	LANGUAGE / SEMANTICS OF INFORMATION	2	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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
C1.4	INFORMATION TIMELINESS	2	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
C1.5	PRIVACY STATEMENT	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.
C1.6	RFID EMBLEM	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.
C1.7	PURPOSE SPECIFICATION	3	A clearly specified purpose for the collected data is available in two versions: one very detailed one including system and

Control code and name		Highest overall category	Description
			application details for the involved employees of the operator 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 trainings, to increase their awareness.
C1.8	ENSURING LIMITED DATA PROCESSING	3	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
C1.9	ENSURING PURPOSE RELATED PROCESSING	3	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. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more.

Control code and name		Highest overall category	Description
			Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
C1.10	ENSURING DATA MINIMISATION	3	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguard from [BSI2009]: **MS17** "Satisfying the data minimization obligation": "Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 77)
C1.11	ENSURING TAG PROTECTION	2	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguard from [BSI2009]: **MM8** "Introduce proximity technology as defined by ISO/IEC14443": "Introduce proximity technology as defined by ISO/IEC14443." (p. 83)

Control code and name		Highest overall category	Description
C1.12	ENSURING PERSONAL DATA QUALITY	2	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.
C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
C1.14	ENSURING DATA ACCURACY	2	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.
C1.15	ENABLING DATA DELETION	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. Related safeguard from [BSI2009]: **MS17** “Satisfying the data minimization obligation”: “Data minimization must be satisfied in accordance with the applicable legal regulations on privacy. Satisfying legal requirements: - When the processes and system as a whole are being defined, the principle of data minimization is applied in accordance with the legal foundations. This requires in particular the definition of deadlines for deletion of data that isn't needed any more. Special safeguards: - Precise, purpose-related definition of data content; data and access/usage rights are acquired and stored using the role model of the system as a whole. - The customer is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people.” (p. 77)
C2.1	OBTAINING DATA SUBJECT'S CONSENT	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.
C4.1	PROVIDING INFORMATION	2	At the time of data collection, the data subject has access to

Control code and name		Highest overall category	Description
	PROCESSING INFORMATION		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 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.
C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1	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: - 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. 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.
C5.2	LOGGING ACCESS TO PERSONAL DATA	2	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2	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 subject's request. These requests are then individually processed and the respective

Control code and name		Highest overall category	Description
			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.
C7.1	SECURITY CONTROLS	---	See relevant controls from TG 03126-1.
C8.1	NOTIFICATION OF AUTHORITY	2	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 weeks prior to the RFID application's launch.
C8.2	PRIOR CHECKING	2	It is ensured that the legally required checking of the RFID application is executed by expert personnel.

Table 47: Public transport PIA – Consolidated view of identified controls

3.2.6 Step 6: Documentation of residual risks

For technical or business reasons it is not always possible to eliminate threats completely by applying controls. Some residual risks remain. These residual risks should be documented in this step. It is recommended to provide a comprehensive description and an evaluation (low, medium, high) for each residual risk.

4 Automotive Scenario

4.1 Initial analysis

For the initial analysis, the decision tree shown in Figure 1 is used. For the current scenario, the answer to Q1 is: Yes, the RFID application does process personal data. Personal data is stored in the following forms:

- user accounts in the access control management system,
- employee accounts in the human resource management system,
- IDs and delivery addresses in the distribution management system,
- customer data in the car dealer management system.

The answer to Q2a is open to some interpretation: If the answer is based solely on the definition of personal data in the Directive 95/46/EC, RFID tags used in the application do not contain personal data. Consequently, the resulting level of PIA analysis is 2 and a full scale PIA is required. If, however, the answer to this question is based on the definition of personal data from Directive 95/46/EC **as well as** WP 136 [ART2007] and WP 175 [ART2010], then RFID tags used in the application do contain personal data. This is the case for the employee access control cards and for the tagged cars. Thus, the resulting level is 3 and a full scale PIA is required. As a result, the manufacturer operating the current scenario is at level 3 of the PIA analysis and needs to conduct a full scale PIA.

Both answers to Q2a require a full scale PIA.

4.2 Risk assessment

The following description of a risk assessment is an exemplary execution of a PIA. A PIA that is conducted by a different group of stakeholders may lead to different conclusions. In particular, the context descriptions and examples in step 2, as well as the reasoning used to derive the demand categories in step 3, might be subjective and are a result of the discussions of the participating stakeholder group. Again, another stakeholder group may come up with different and additional damage scenarios and potential implications. The aim of a PIA is to create a common understanding about the RFID application's privacy implications within the involved stakeholder group and thus facilitates commonly accepted conclusions.

4.2.1 Step 1: Characterisation of the application

4.2.1.1 Systems and entities

4.2.1.1.1 Systems and system components

Figure 52 gives a generic overview regarding the systems and their associated components that form the backend system, which is required to realize the described automotive scenario. Most

likely, the different systems will reside on different locations and will be under the responsibility of different entities. This is indicated in Figure 52 by grouping the systems and their components accordingly.

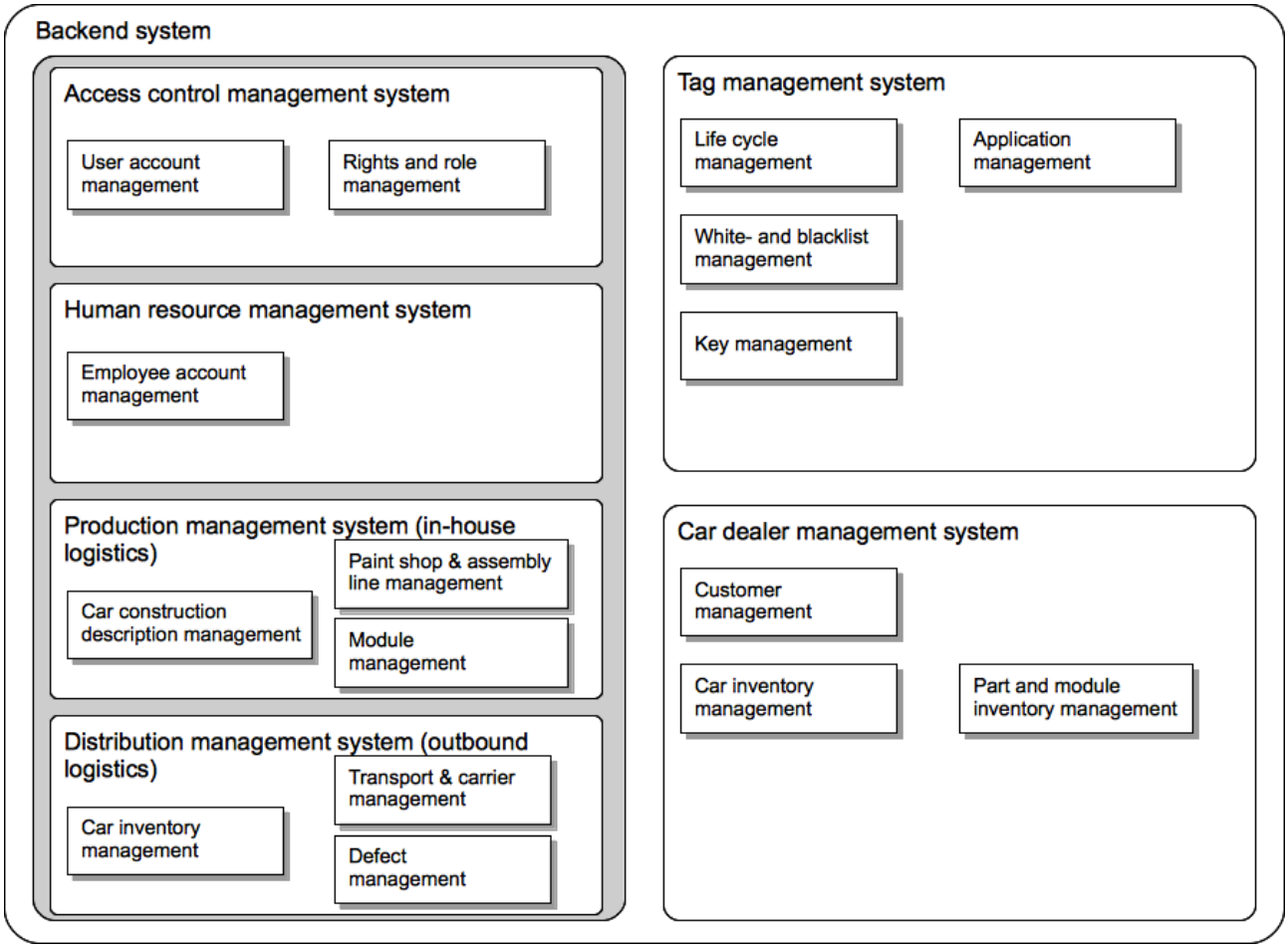

Figure 52: Automotive backend system

The access control management system manages the access to all buildings and facilities on the factory premises. It consists of two main components:

- User account management
  This component provides all necessary functions to create, update and delete user accounts. Each employee has an employee card, which allows him to access the buildings he is working in. Each employee card has an associated user account, which contains all data that is necessary to manage the employee's individual access rights. All changes to a user's initial access rights are recorded, e.g. in the form of a history trail.
- Rights and role management
  This component provides all necessary functions to manage the different access rights and roles that are relevant in the realm of the factory facilities. These rights and roles are assigned to users. Different employees may have different access rights, e.g. an assembly line worker might not have access to research facilities.

The human resource management system deals with all processes that are related to recruiting new employees, employee contracts, salaries, agreement on objectives, holidays, etc. The only main component relevant for the described scenario is:

- Employee account management
  This component provides all necessary functions to manage employee's personal data as well as their job descriptions and working place.

The production management system manages all processes that are related to in-house logistics. Amongst others, it consists of the following three main components:

- Car construction description management
  This component provides all necessary functions to manage the individual construction descriptions of the cars. These descriptions contain all details that are necessary to construct the car – starting with the car body and the paint shop requirements, ending with the necessary modules and parts to assemble the individual car.
- Paint shop and assembly line management
  This component provides all necessary functions to steer the paint shop processes and the assembly line. This includes the management of the machines, tools, materials, modules and parts.
- Module management
  This component provides all necessary functions to manage and track all tagged security-relevant and upscale modules.

The distribution management system manages all processes that are related to outbound logistics. Amongst others, it consists of the following two main components:

- Car inventory management
  This component provides all necessary functions to manage the whereabouts of the cars, which are ready to deliver, on the factory premises.
- Transport & carrier management
  This component provides all necessary functions to manage target location, transport dates, etc. for each individual car as well as the transfer of the cars on the factory premises and the transport to the car dealers/customers with the help of specialised carriers.
- Defect management
  This component provides all necessary functions to manage defect reports that have been created by car dealers and resulting recall activities.

As there are different carrier mediums utilized throughout the described automotive scenario, these are summarized under the term “tag”. In the detailed use case descriptions, the term “tag” is then specified with prefixes, e.g. employee card tag, car body tag, car tag or module tag.

The tag management system provides the functions and processes that are needed to manage the tags regardless of the relevant carrier medium. It consists of four main components:

- Life cycle management
  This component provides all necessary functions to personalise, configure and change the tag with the contact-less interface.
- White- and blacklist management
  This component provides all necessary functions to provide, update and distribute white- and blacklists of tags as well as applications.
- Key Management
  This component encloses all relevant security parameters and cryptographic keys. Key management procedures work as described in 7.12 of [BSI2010].

- Application Management
  This component provides all necessary functions to provide, update and withdraw applications.

The car dealer management system deals with all processes that make up a local car dealer, e.g. customer management, repair shop management, inventory management, supplier management etc. The following three main components are relevant for the described scenario:

- Customer management
  This component provides all necessary functions to manage customers' personal data, orders and repair dates.
- Car inventory management
  This component provides all necessary functions to register the reception of cars, which are for sale or need to be repaired. Thus, all cars that the car dealer is responsible for at a certain time.
- Part and module inventory management
  This component provides all necessary functions to realise the timely ordering of parts and modules and stock monitoring.

4.2.1.1.2 Entities and their roles

The following entities have been identified to be relevant for the described retail scenario:

- Employee
  A person who is employed by the manufacturer and who works on the factory premises. Each employee is the holder of an employee card. The employee is identical to the one described in [BSI2010], page 23.
- Car manufacturer
  An organisation that mainly develops and manufactures cars on the factory premises. It deals with all relevant stakeholders and owns inbound, in-house and outbound processes. The car manufacturer is identical to the “organisation” described in [BSI2010], page 23.
- Carrier
  An organisation that specialises on the transport of cars. This organisation might be independent from or associated to the car manufacturer. Its management systems are closely linked to the car manufacturer's distribution management system.
- Car dealer
  An organisation that sells and repairs cars on a local basis. This organisation might be independent from or associated to the car manufacturer.

4.2.1.2 Generic business processes

4.2.1.2.1 Process A-P1: Registering for and using an employee access control card

Organisations provide their employees with access control cards, so that they can access their workplaces. For each new employee of the car manufacturer an employee card is requested by the human resource management system and then personalised for the respective employee.

After having received the employee card, the employee can easily access his workplace as well as buildings on the factory premises he is allowed to access. These access rights differ from employee to employee and depend on the employee's job description and responsibilities.

When an employee stops to work for the organisation, he needs to give back his employee card and all his access rights are revoked.

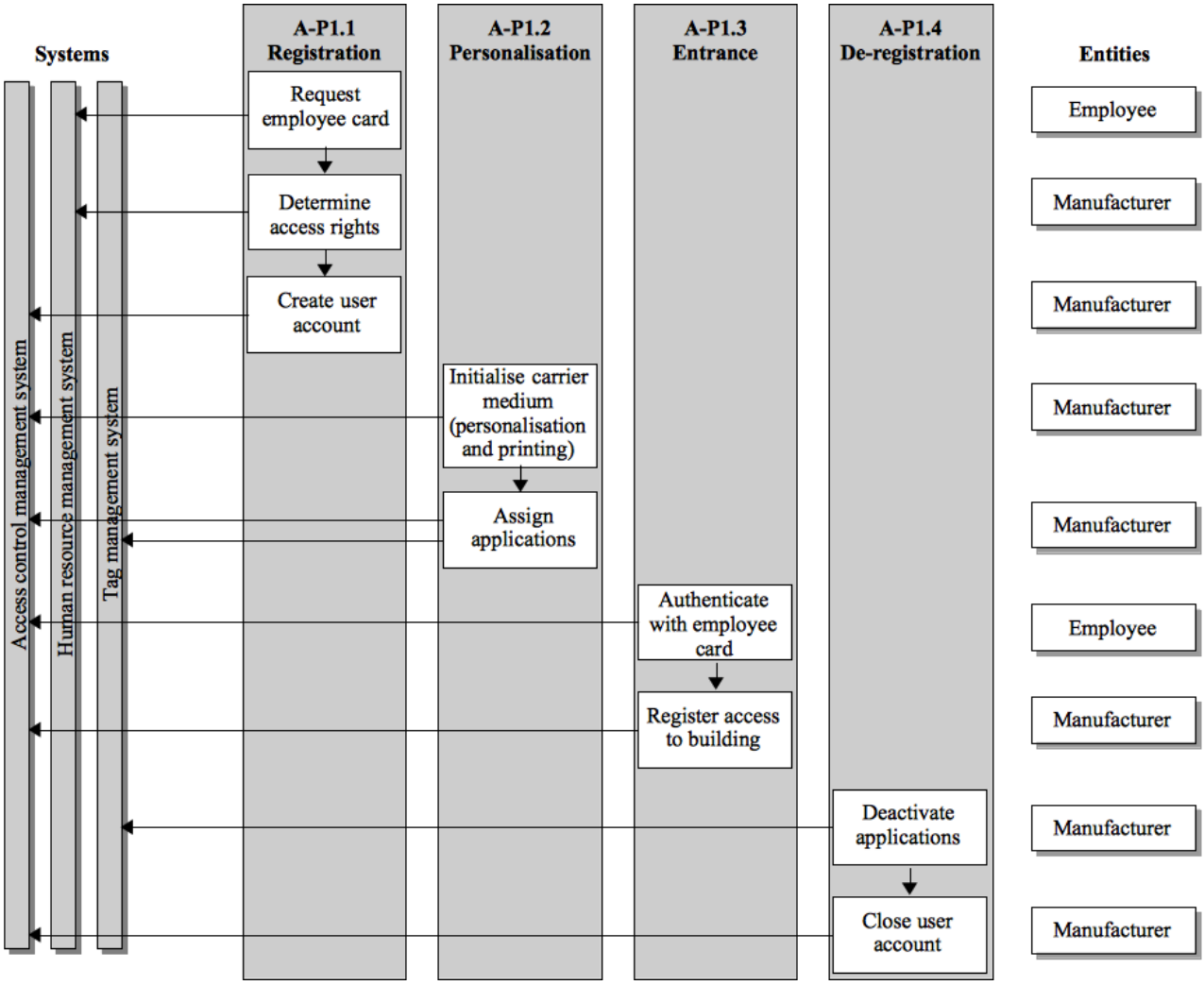

Figure 53: Process A-P1 – Registering for and using an employee access control card

4.2.1.2.2 Process A-P2: Automatically steering the car assembly

RFID technology is used to further automatise, optimise and steer manufacturing processes. In this automotive scenario the focus lies on the following three main manufacturing steps: car body construction, paint shop and assembly line. Furthermore, a data-on-network approach is described, which means that in most cases tags only contain an identifier. This identifier is then used to retrieve detailed information from a backend system.

When the car body has been constructed, a tag is attached to it, which will identify this individual car for its entire lifetime. Because of cost reasons, the tag will be passive, without cryptographic functionality but might be password protected. An individual construction description is then created in the production management system and linked to the tag's ID. This construction description contains all the details that are necessary to finalise the construction of the individual car.

In the paint shop and in the assembly line, this tag is then used to steer the processes according to the individual construction description.

As an individual car might consist of 5000 to 7000 modules and parts, it is not feasible to tag each of these modules and parts. Only so called security-relevant and upscale modules are tagged. The tagging happens either at the supplier or at the manufacturer. The tag will be passive, without cryptographic functionality and might contain some additional quality-related information. These tags can later be used e.g. for recall and plagiarism cases.

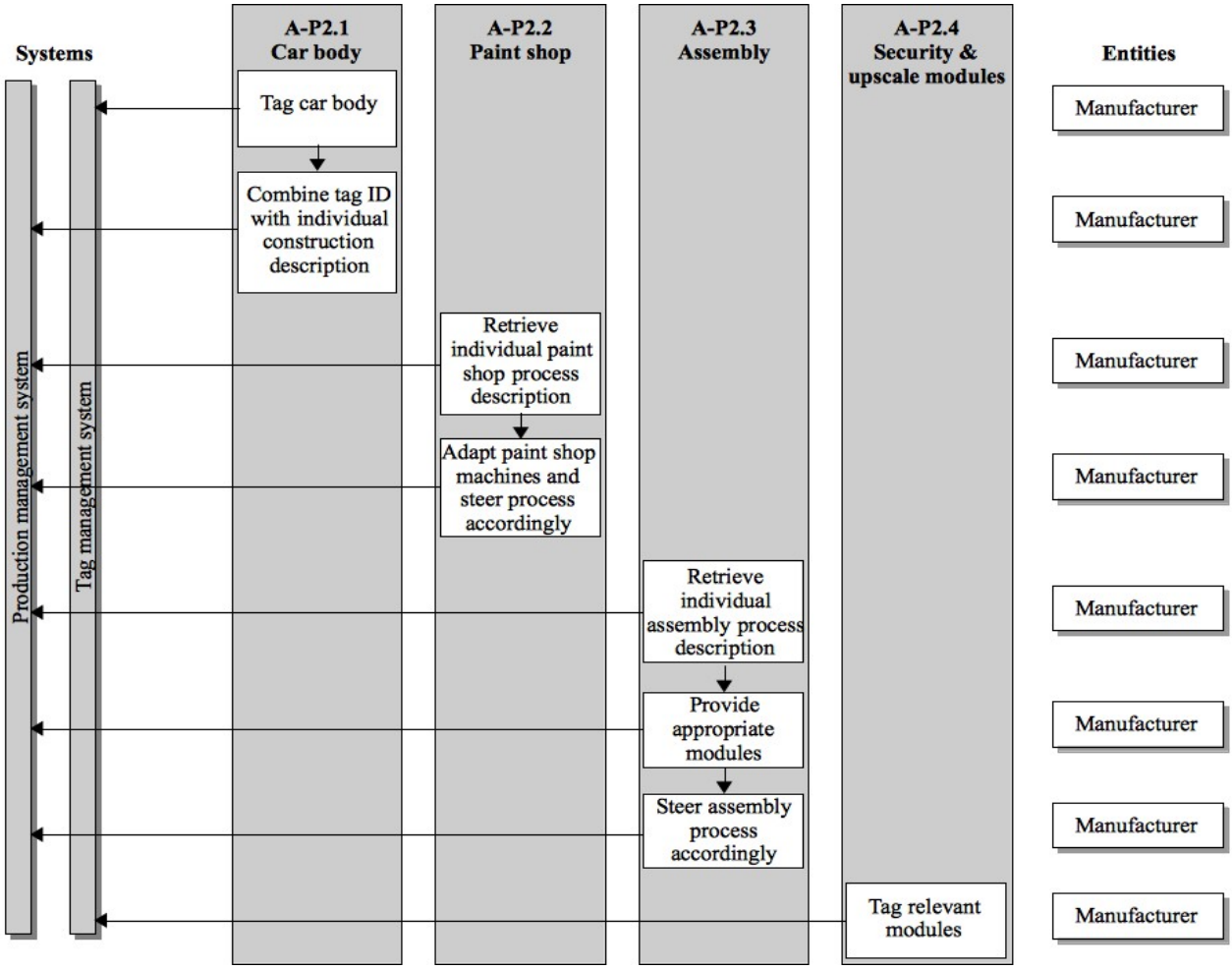

Figure 54: Process A-P2 – Automatically steering the car assembly

4.2.1.2.3 Process A-P3: Localising and distributing cars

As described earlier, the car body tag is used as a lifetime identification. As such it is also used to manage the transfer of the cars on the factory premises as well as the transport to the car dealers and customers. Again, the detailed information to steer these processes resides in a backend system – the distribution management system – and the tag is only used to localise and identify the individual car.

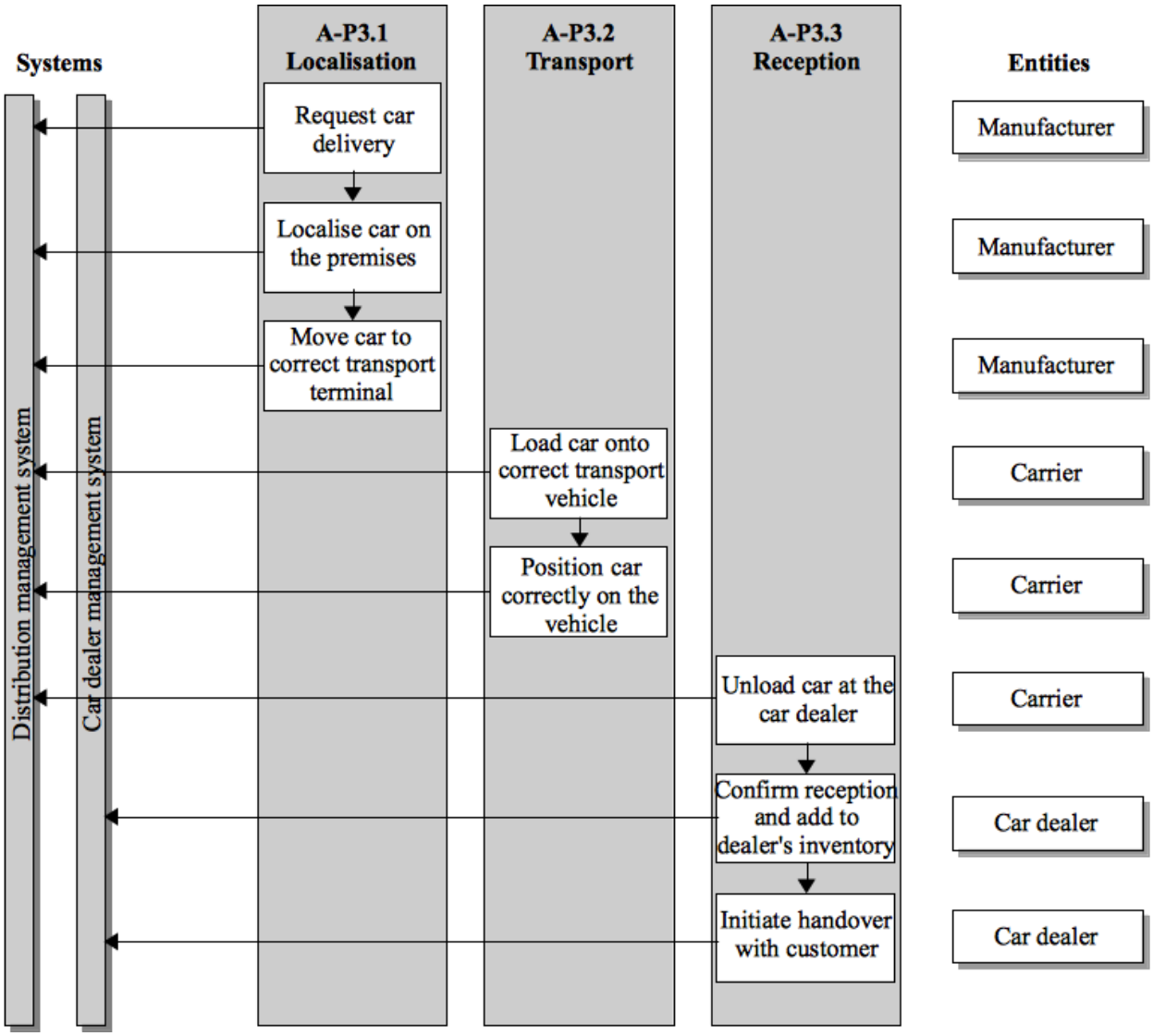

Figure 55: Process A-P3 – Localising and distributing cars

4.2.1.2.4 Process A-P4: Initiating a recall process

In the case of an accident or a defective module, the earlier described module tags can be read at the car dealer. This identity as well as the present defect can then be handed over to the manufacturer. The manufacturer – together with affected suppliers – investigates the defect and initiates a recall if necessary. Based on the module tags, the individual construction descriptions and the car body tags, affected car dealers and customers can be informed about the recall.

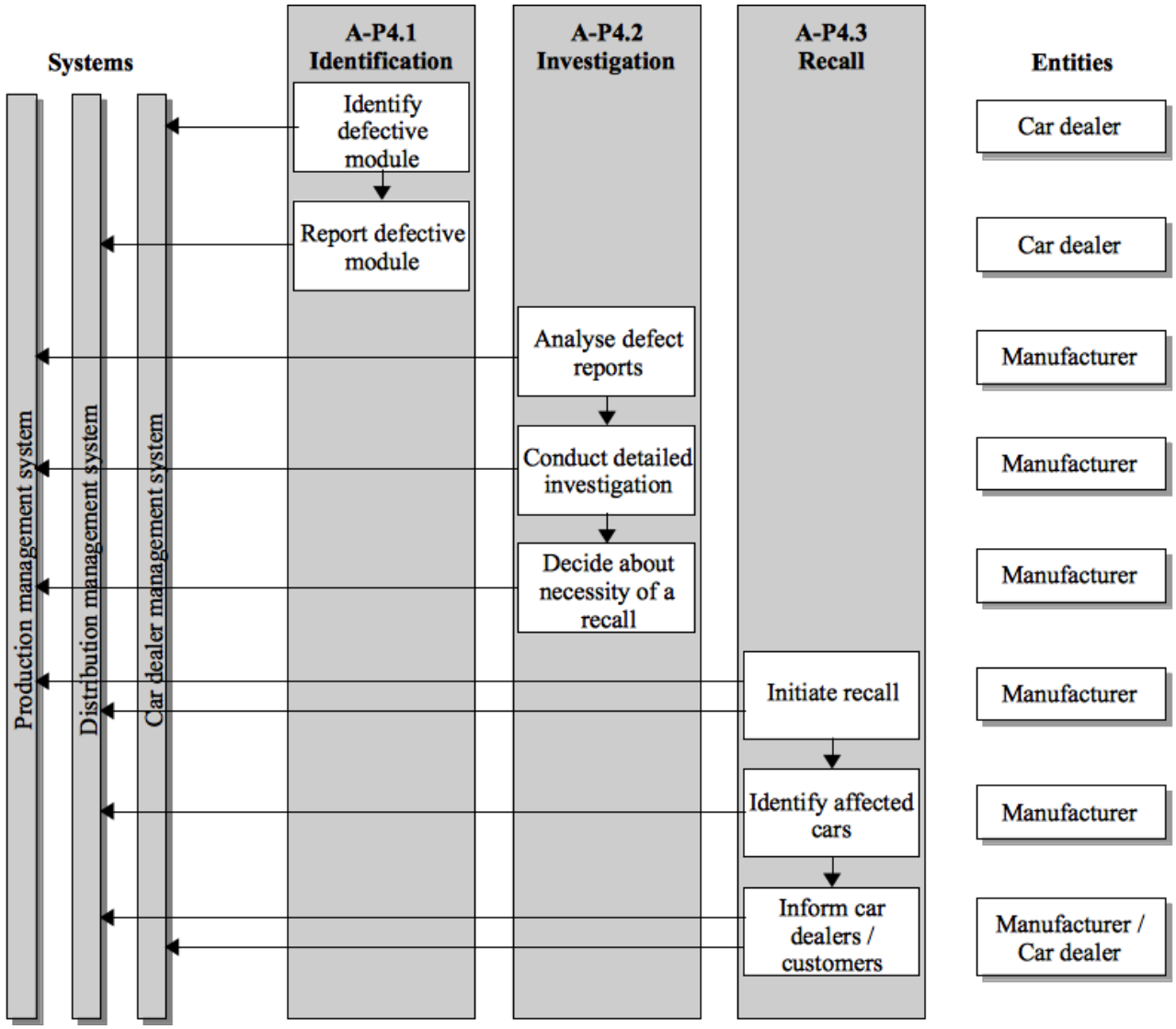

Figure 56: Process A-P4 – Initiating a recall process

4.2.1.3 Use cases

4.2.1.3.1 Use case A-UC 1.1: Registering for an employee card

The request for a new employee card is available. Thus, either a new employee has started to work for the manufacturer or an existing employee lost or damaged his card and needs a new one. Consequently, the employee's data is retrieved from his employee account in the human resource management system and it is checked whether a new or a replacement employee card needs to be provided. In the latter case, all necessary data for the personalisation is already available and the personalisation is initiated.

If a new employee card is needed, it is necessary to determine the individual access rights as well as the validity timeframe. This is done based on job profile and contract information from the employee's account in the human resource management system as well as generally defined access

rights and role rules in the access control management system. With this information a user account is created in the access control management system. Then the employee card's personalisation is initiated and a respective entry is written to the employee account in the human resource management system.

This use case combines “Identification of employee” and “Create user account or retrieve already existing user account” use cases from [BSI2010], page 49. Nevertheless, it describes the procedure from a slightly different perspective, namely omitting the identification process and focussing on data exchange between affected systems.

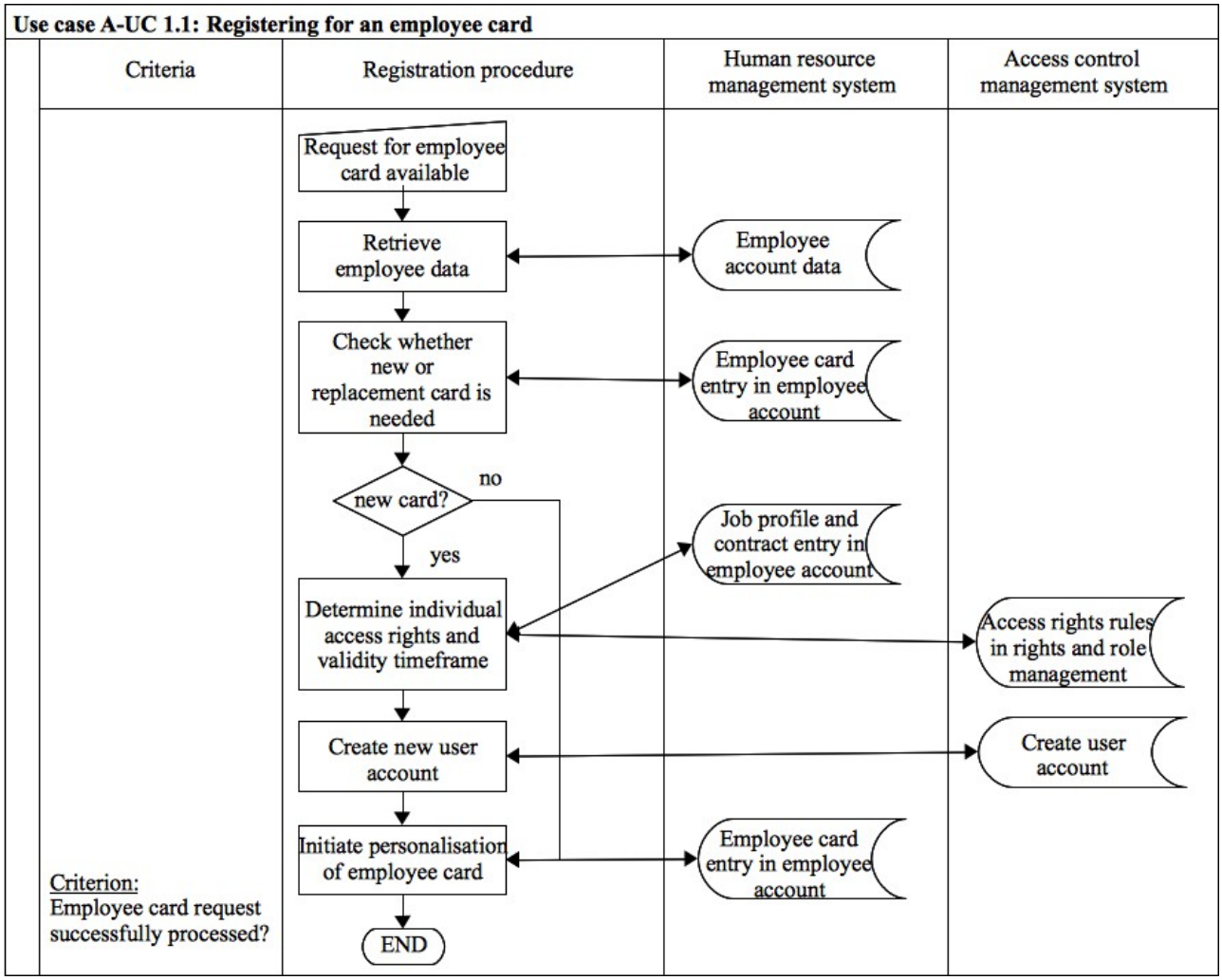

Figure 57: Use case A-UC 1.1 – Registering for an employee card

4.2.1.3.2 Use case A-UC 1.2: Personalising the employee card

The order request for an employee card is processed by the access control management system. A new employee card is initialised with an ID and the relevant access rights and roles, the ID is then registered in the respective user account. If there is the need for distinct card applications, these are initialised and registered in the user account, too. Finally, the employee's name and/or his photo are printed onto the employee card.

This use case deals with the same topic as “Initialisation of the carrier medium” from [BSI2010], page 50 ff. Nevertheless, it describes the personalisation procedure from a slightly different perspective, namely omitting some of the technical details and focussing on privacy relevant aspects.

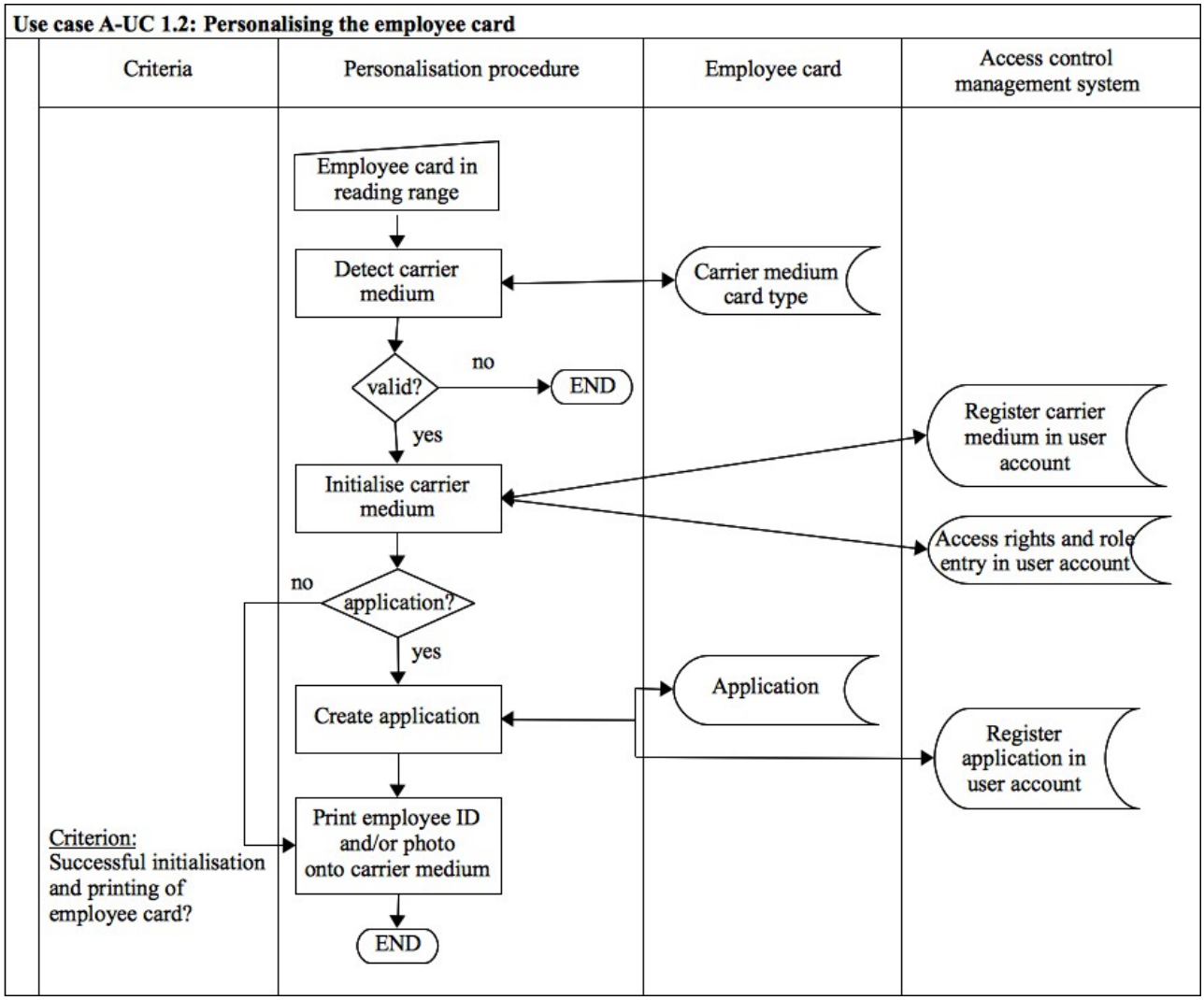

Figure 58: Use case A-UC 1.2 – Personalising the employee card

4.2.1.3.3 Use case A-UC 1.3: Entering or leaving a building

When an employee wants to enter or leave a building, he needs to provide his employee card. Holding his ticket to the reader, it

- might be necessary to enter an authentication factor
  In this case, the employee needs to enter e.g. a PIN, a password or his fingerprint. Performing such an authentication guarantees that an employee card can only be used by the respective employee.
- or not
  In this case, the employee only needs to hold the employee card in front of the reader.

Then the validity of the employee card is checked against the black- and whitelists in the tag management system. If it is not valid, the procedure ends and access to the building is not granted to the employee. If it is valid, the respective user data is retrieved from the user account in the access control management system and an authentication entry is written to the user account. This authentication entry contains the user's ID, the door ID and a timestamp.

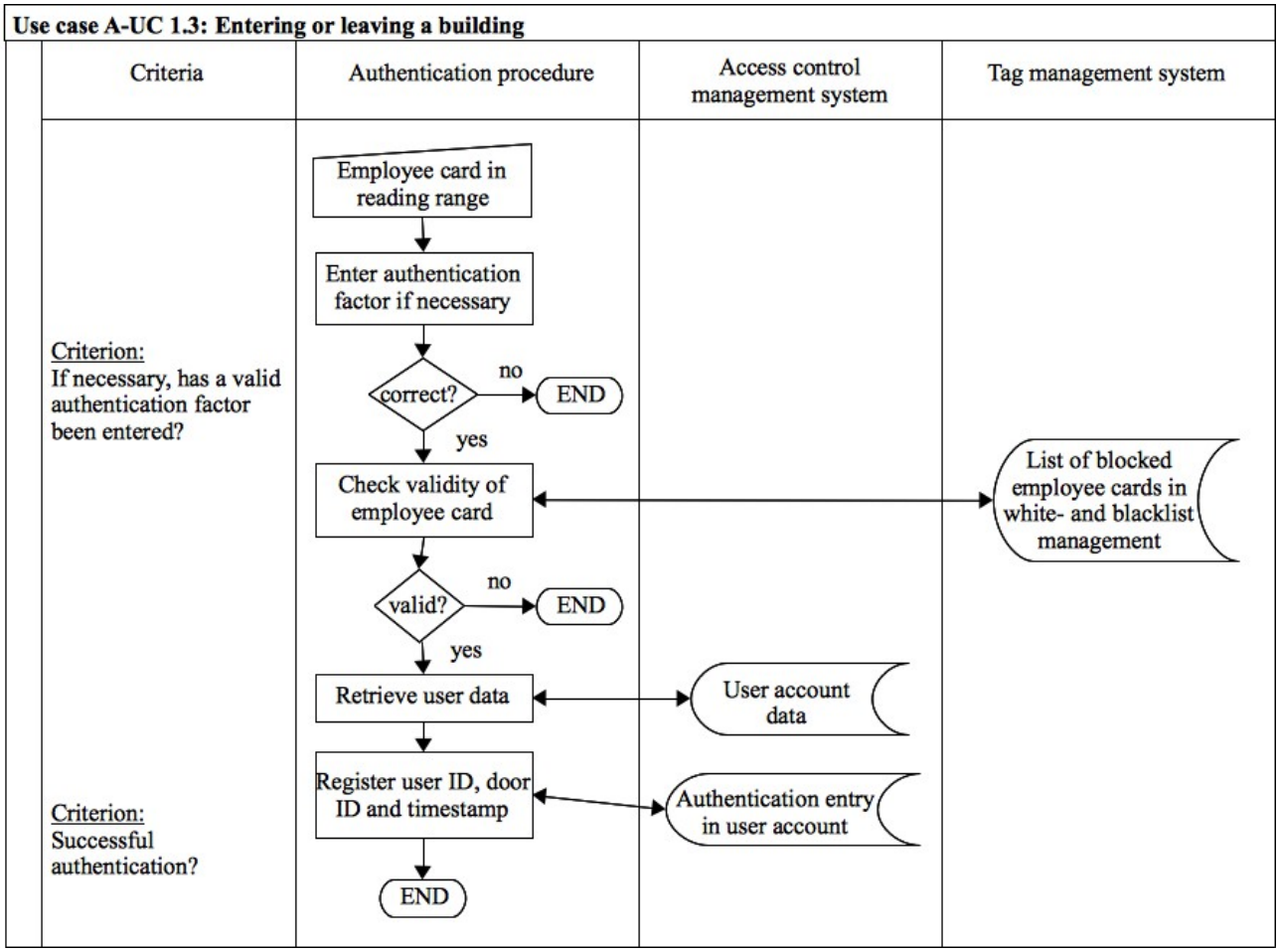

Figure 59: Use case A-UC 1.3 – Entering or leaving a building

4.2.1.3.4 Use case A-UC 1.4: De-registering an employee card

The prerequisite for this use case is the application of an employee for a de-registration. The de-registration request is only accepted and filed for further processing after positively identifying the employee.

When a de-registration request has been filed, the respective data is retrieved from the user account in the access control management system. If there are any card applications registered in the user account, these are blocked and the application-specific black- and whitelists are updated accordingly. In the next step the employee card itself is blocked and the carrier medium-specific black- and whitelists are updated accordingly. Consequently, the employee cannot use his employee card anymore.

The next step of the de-registration procedure is to add a de-registration entry to the user account and to the employee account in the human resource management system. Then it needs to be

checked whether the user account has to be deleted. If it does not contain any personal data or references to personal data its data could be saved by the car manufacturer and further used for analysis purposes. If the user account contains personal data or the car manufacturer does not want to keep the data, the deletion of the user account is scheduled. Now starts a dedicated period of time during which the de-registration request could be taken back e.g. in the case that the employee's contract has been prolonged. Only when this period of time elapses, the actual deletion of the user account is performed.

This use case deals with the same topic as “Deregistration” from [BSI2010], page 64. Nevertheless, it describes the de-registration procedure from a slightly different perspective, namely omitting some of the technical details and focussing on privacy relevant aspects.

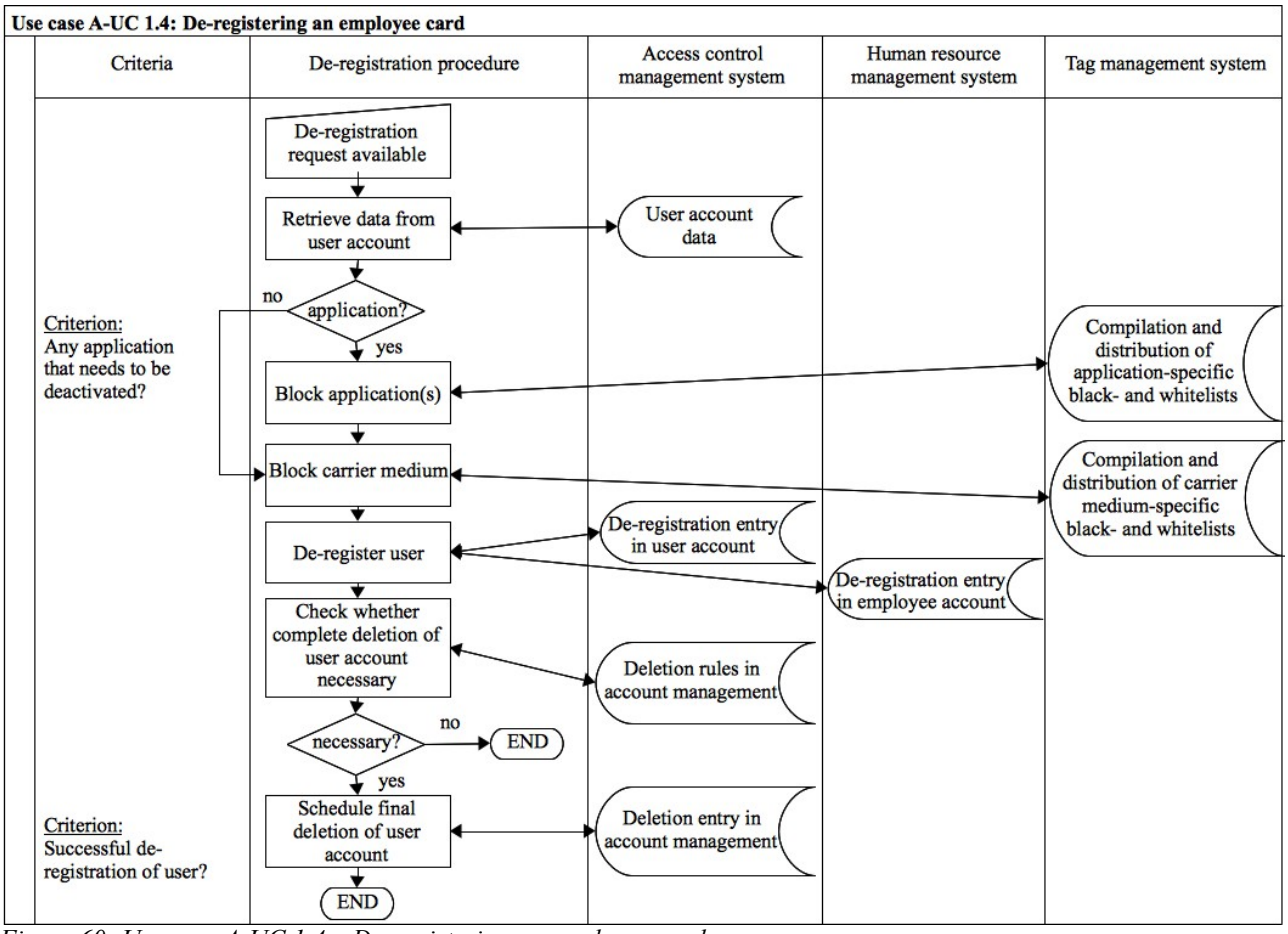

Figure 60: Use case A-UC 1.4 – De-registering an employee card

4.2.1.3.5 Use case A-UC 2.1: Tagging a car body

When the car body has been finalised a tag is attached to it. This tag is then initialised and its ID is registered in the car's individual construction description that resides in the production management system. This individual construction description is then checked for completeness, which means that it at least contains complete paint shop and assembly process descriptions. If completeness has been assured the tagging procedure is finalised and the completion of the car body construction process is logged in the individual construction description.

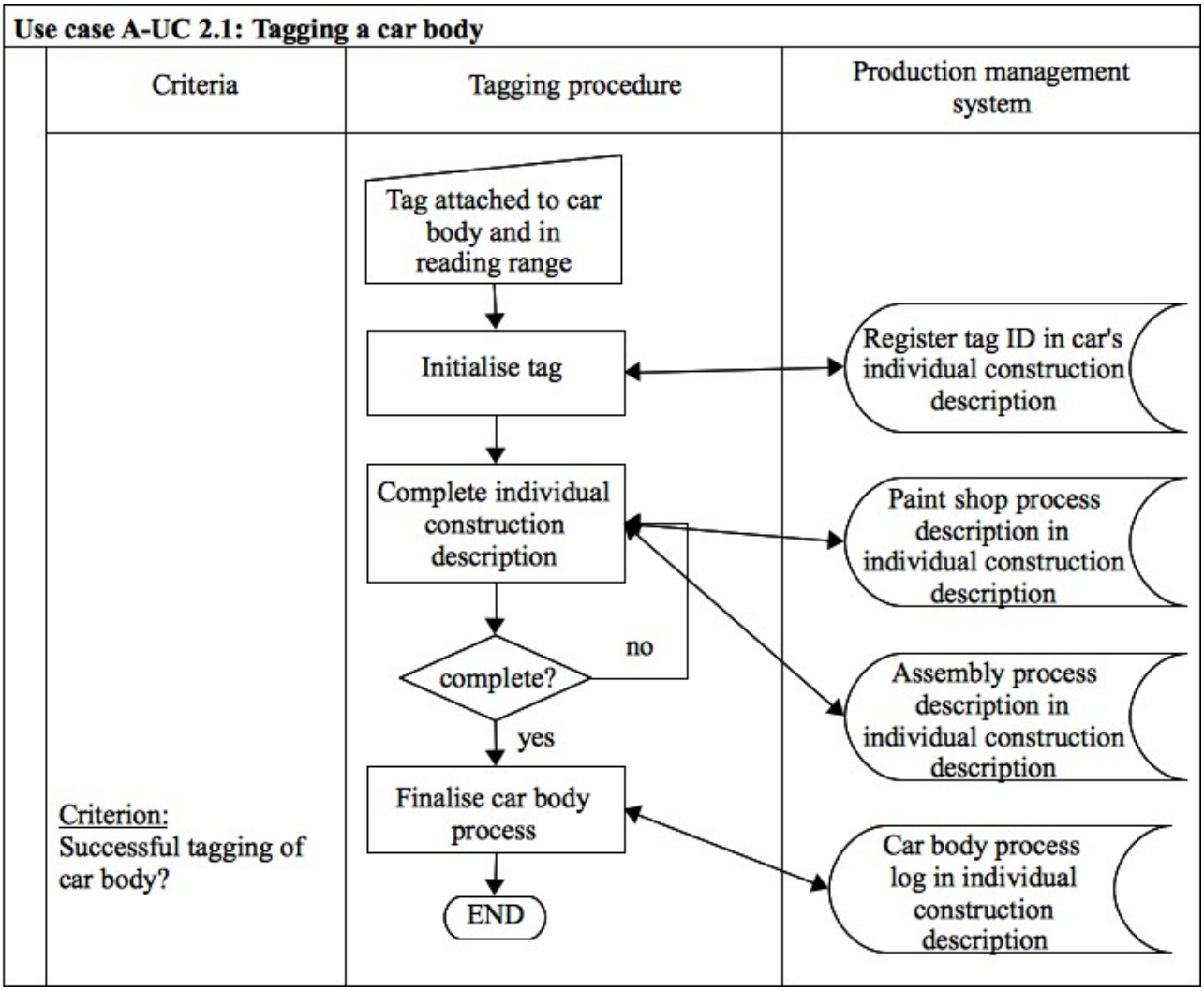

Figure 61: Use case A-UC 2.1 – Tagging a car body

4.2.1.3.6 Use case A-UC 2.2: Automatically steering paint shop processes

When a car body enters the paint shop its tag is read and the car's individual construction description is retrieved from the production management system. The description is checked for individual requirements that need to be realized in the paint shop.

Then the paint shop process description is retrieved and the paint shop, namely its processes, machines and relevant materials are adapted accordingly. The execution of processes follows. If the execution is not successful, an error process is initiated. If the execution is successful, the paint shop process is finalised and the completion of the paint shop process is logged in the individual construction description.

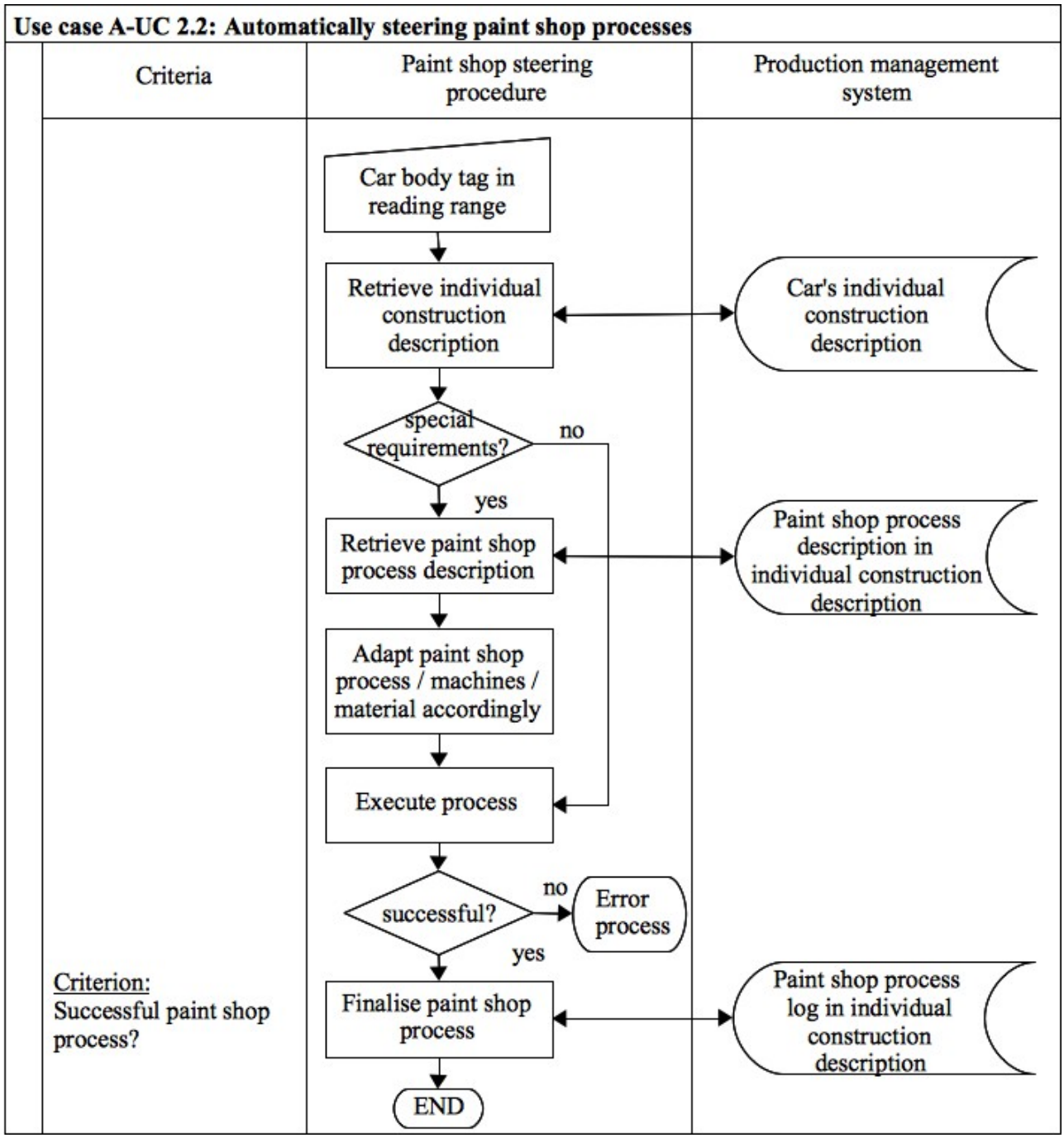

Figure 62: Use case A-UC 2.2 – Automatically steering paint shop processes

4.2.1.3.7 Use case A-UC 2.3: Automatically steering assembly processes

When a painted car body enters the assembly line its tag is read and the car's individual construction description is retrieved from the production management system.

Then the assembly process description is retrieved and it is checked whether the appropriate modules and parts are available. If there are modules missing, an error process is initiated. If all

relevant modules are available, the assembly line, namely its processes and machines are adapted according to the assembly description.

The execution of processes follows. If the execution is not successful, an error process is initiated. If the execution is successful, the assembly process is finalised and the completion of the assembly process is logged in the individual construction description.

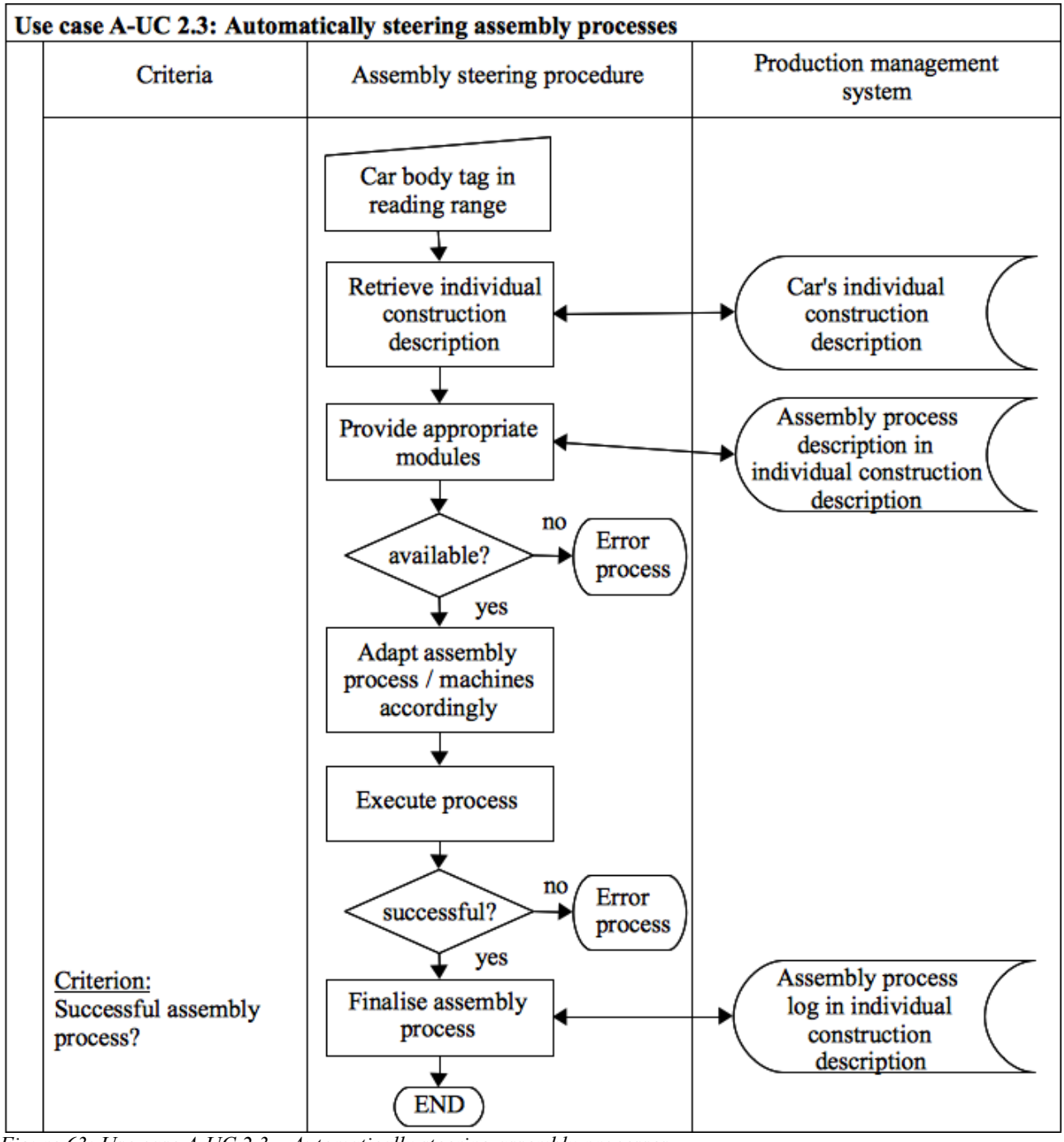

Figure 63: Use case A-UC 2.3 – Automatically steering assembly processes

4.2.1.3.8 Use case A-UC 2.4: Tagging of security-relevant and upscale modules

As described earlier, security-relevant and upscale modules are either tagged by the supplier or by the manufacturer. In both cases, after delivery or initialisation, tag IDs and respective module information are centrally stored in the production management system.

When a tagged module is built into a car body during assembly, the module tag's ID is registered in the car's individual construction description.

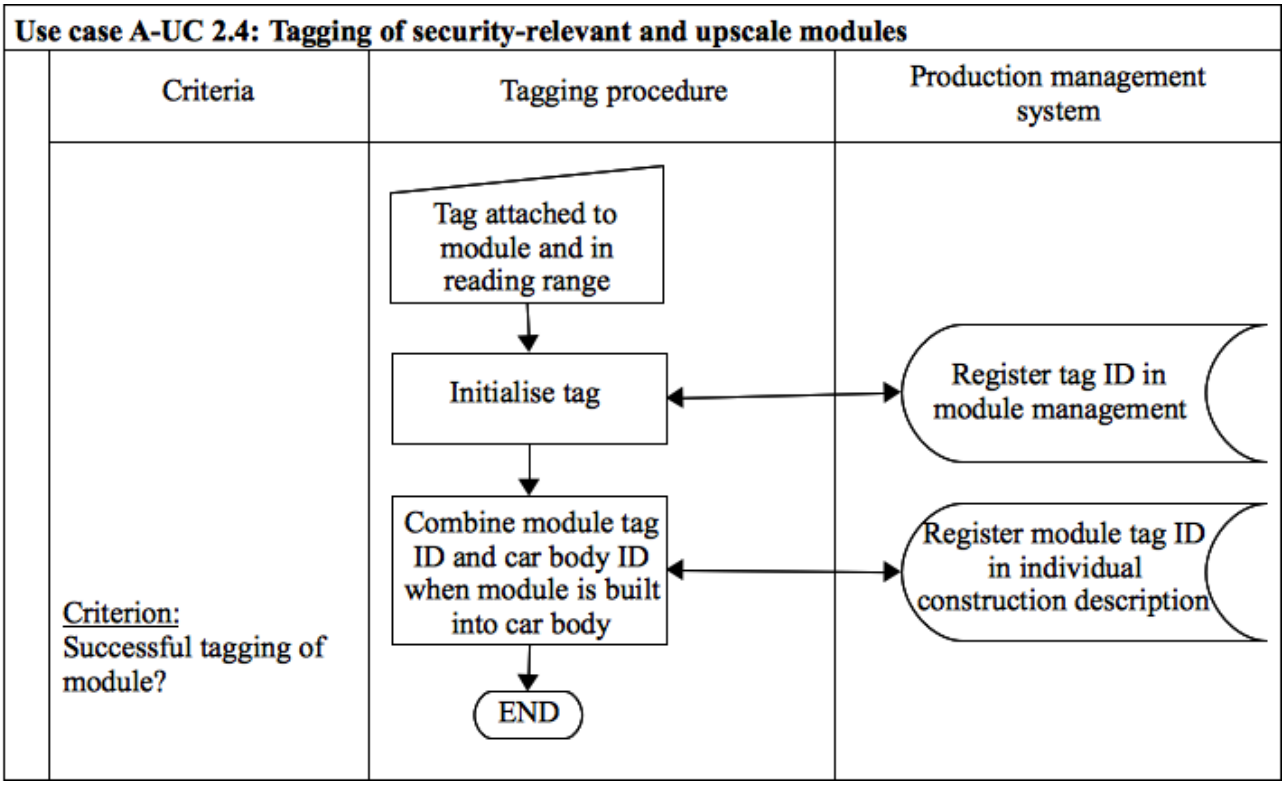

Figure 64: Use case A-UC 2.4 – Tagging of security-relevant and upscale modules

4.2.1.3.9 Use case A-UC 3.1: Localising a car on the factory premises

The distribution management system gets the request to deliver a distinct car. The car's parking space/position on the factory premises is retrieved from the inventory management. This position is verified by actually localising the car with the help of its tag and readers that are positioned on the parking space. If the car cannot be localised at the given space/position, all other parking spaces on the factory premises are searched.

If the car has been successfully localised, its transfer to the appropriate transport terminal is requested. This can either be a train or truck terminal. To identify the correct terminal, the terminal ID is retrieved from the distribution management system, which holds all the information that is necessary to transfer the car to its customer.

After successful transfer to the transport terminal, the car's reception is registered in the distribution management system.

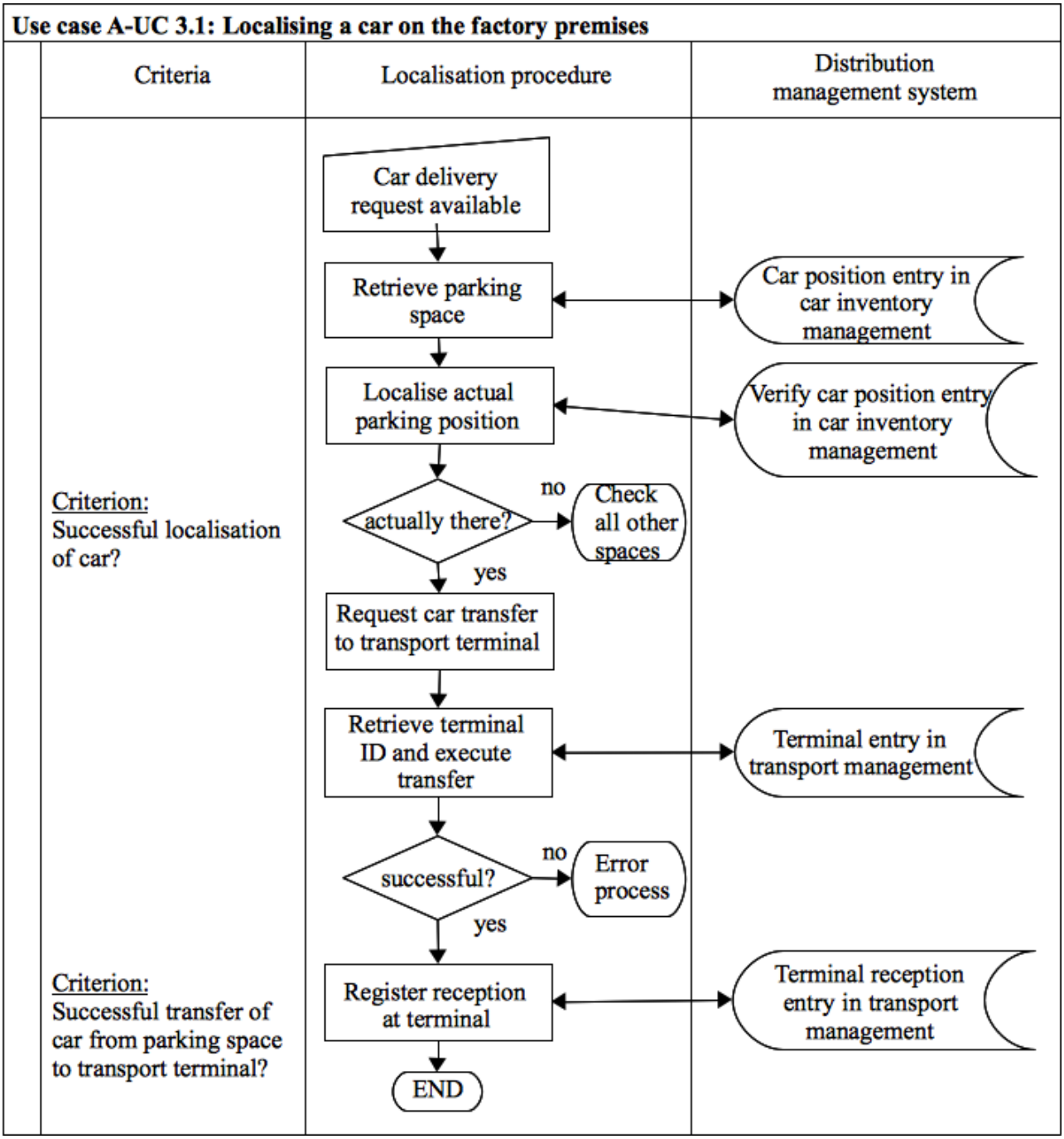

Figure 65: Use case A-UC 3.1 – Localising a car on the factory premises

4.2.1.3.10 Use case A-UC 3.2: Loading a car on a transport vehicle

At the transport terminal, the car needs to be loaded onto the transport vehicle. To do this properly, target location of the car and matching transport vehicle ID are retrieved from the distribution management system. If this information is not a available, an error process is initiated. If it is available, the car is transferred to the correct vehicle.

Then the defined car's position on the vehicle is retrieved. Again, if this is not available, an error process is initiated. If it is available the car is positioned correctly on the vehicle. Finally, the loading procedure is finished and a successful loading entry is written to the distribution management system.

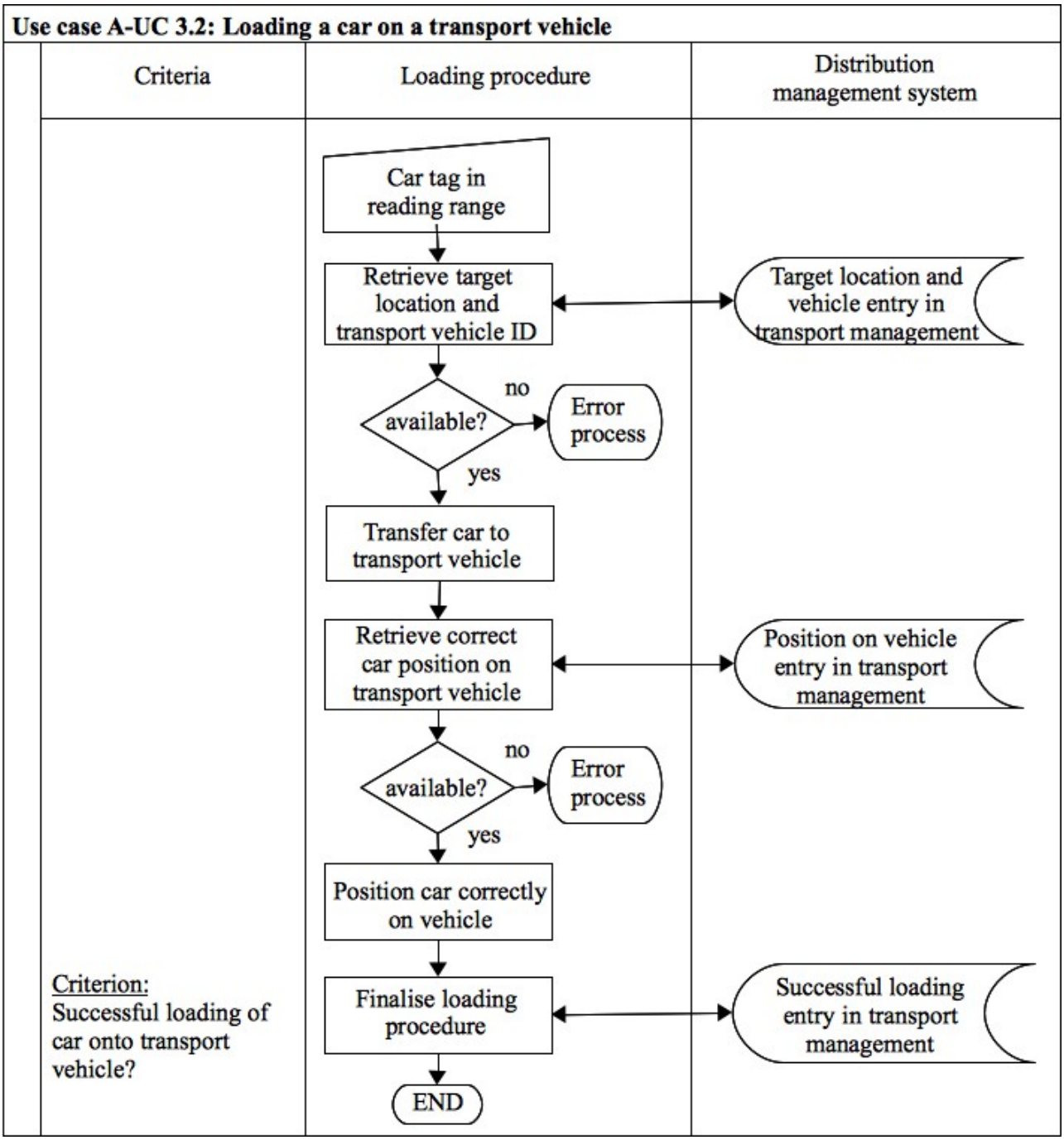

Figure 66: Use case A-UC 3.2 – Loading a car on a transport vehicle

4.2.1.3.11 Use case A-UC 3.3: Receiving a car at the car dealer

When the transport vehicle arrives at the car dealer, the car tag is read and the car's target location is retrieved from the distribution management system. It is checked whether the given target location equals the present car dealer. If both locations are not equal, the unloading and reception procedure aborts. If it is the correct dealer, the car is unloaded and it's reception is confirmed by the car dealer. A respective reception confirmation is written to the distribution management system and a reception entry is written to the inventory management of the car dealer.

Based on the order entry in the customer management of the car dealer, a handover is initiated with the customer.

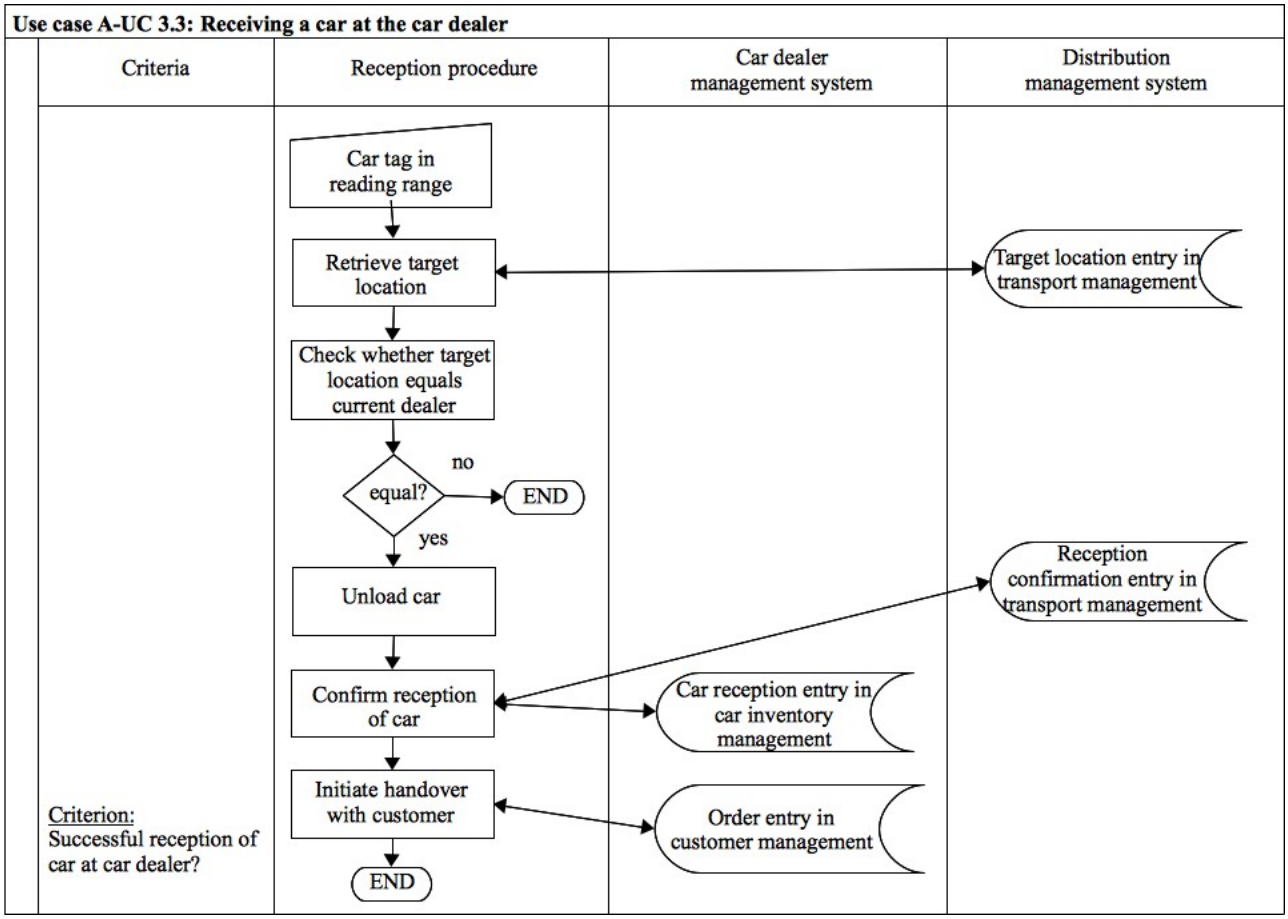

Figure 67: Use case A-UC 3.3 – Receiving a car at the car dealer

4.2.1.3.12 Use case A-UC 4.1: Identifying a defective security-relevant/upscale module

As described earlier, in the case of an accident or a defective module, the module tags can be read at the car dealer. Detailed module information is retrieved from the car dealer's inventory management and with the help of defined rules, the defect's severity can be categorised. A defect report, which contains the module's ID, a defect description, a severity category and the car's ID, is sent to the manufacturer and written to the distribution management system.

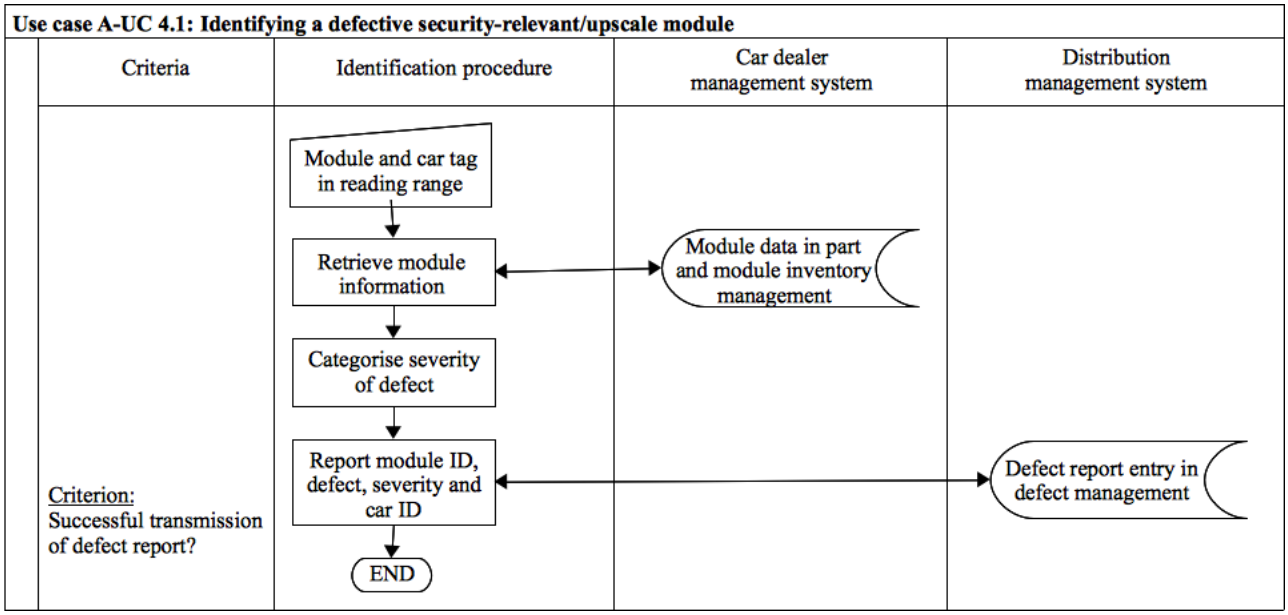

Figure 68: Use case A-UC 4.1 – Identifying a defective security-relevant/upscale module

4.2.1.3.13 Use case A-UC 4.2: Investigating a defect

At the manufacturer, the defect reports from the distribution management system are combined with module IDs and respective detailed information, and thus sorted and aggregated by module type. Then the manufacturer and affected supplier conduct a detailed investigation and decide whether a recall is necessary or not. If no recall is necessary, the procedure finishes. If a recall is necessary, the recall decision is registered in the production management system and in the distribution management system.

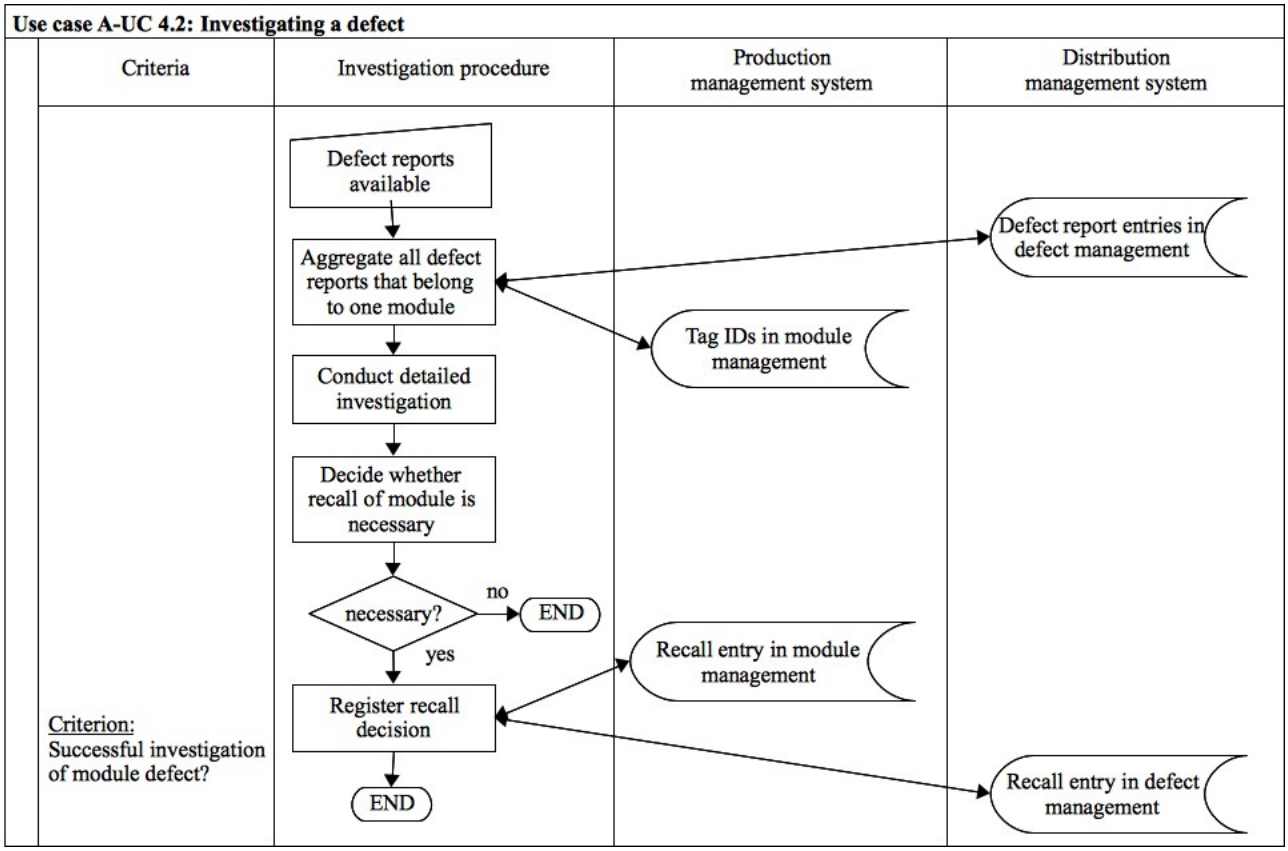

Figure 69: Use case A-UC 4.2 – Investigating a defect

4.2.1.3.14 Use case A-UC 4.3: Initiating a security-relevant/upscale module recall

When a recall decision has been made, all affected module instances are identified with the help of of the module tag's IDs and detailed information that has been stored in the production management system (see A-UC 2.4).

Based on the identified module IDs, all affected cars are identified, as the module IDs have been stored in the car's individual construction description in the production management system (see A-UC 2.4).

Then, with the help of the target locations in the distribution management system, all affected car dealers and customers can be identified. Car dealers are then informed about the recall. A respective recall entry is written to the customer management of the car dealer and the respective customer is informed, too.

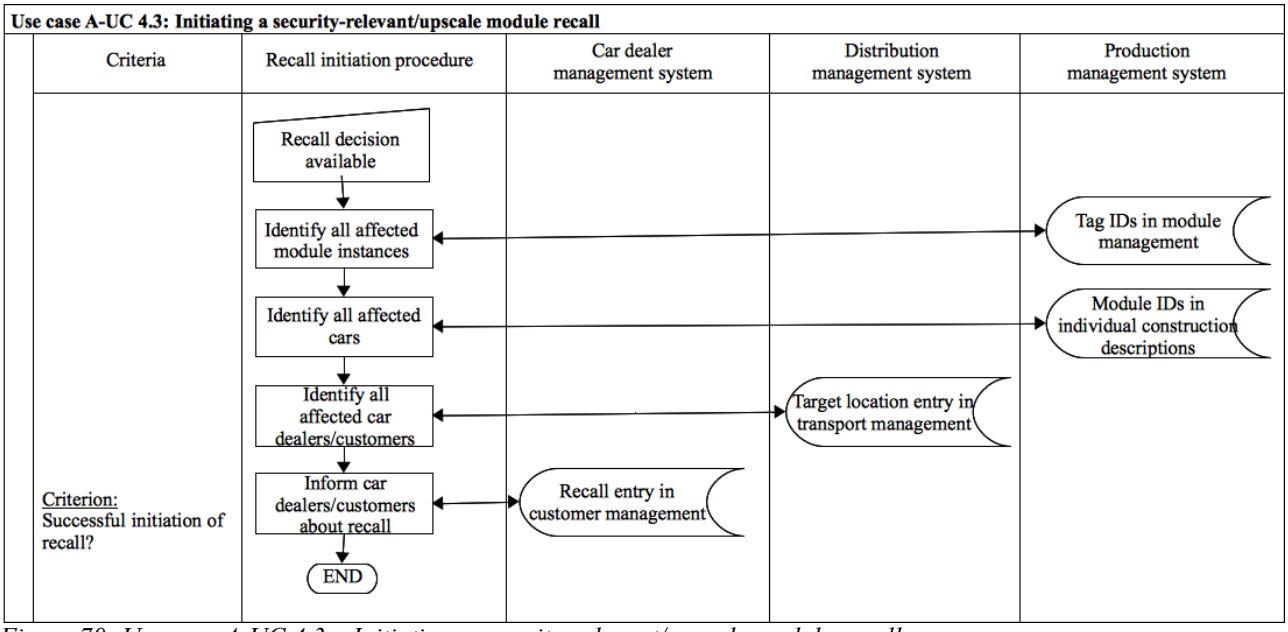

Figure 70: Use case A-UC 4.3 – Initiating a security-relevant/upscale module recall

4.2.2 The employee access control card

4.2.2.1 Step 2: Definition of privacy targets

In this step, stakeholders should discuss the privacy targets that are described in the PIA Framework and the concrete instances of those privacy targets as described in the PIA guideline. By discussing the targets and their instances, stakeholders can clarify what the targets mean in the context of the specific RFID application and corresponding business cases.

Privacy target code and name		**Contextual explanation**	**Examples for how to reach this target**
P1.1	Ensuring fair and lawful processing through transparency	The employees need to know how the RFID technology used in the access control system produces data flows related to them entering and exiting buildings. The information should be prepared in an understandable and easily accessible way.	Give informational material to each employee who gets the access card for the first time. Also provide this information on intranet pages. Human resource personnel should be trained, too.
P1.2	Providing purpose specification and limitation	The operator must explicitly specify why the employee data in the user account of the access control management system and in the employee account of the human resource management system are collected and stored. The purpose should be to enable access control and not to supervise the comings and goings of employees.	Provide clear internal and external purpose specifications. Ensure that access rights are handled accordingly and employees are well informed about what their personal data is used for.
P1.3	Ensuring data avoidance and minimisation	When the operator designs and implements the access control and human resource management systems, he must ensure that only necessary employee data is	Ensure that only employee data that is needed to enable access control on the manufacturers

Privacy target code and name		Contextual explanation	Examples for how to reach this target
		collected and processed. In this context, necessary means that the data is needed for the fulfilment of the specified purpose.	premises is stored in the user account of the access control system.
P1.4	Ensuring quality of data	The operator must regularly check employee data that is stored in access control and human resource management systems to ensure that it is correct and up-to-date. Correct access control heavily depends on the accuracy of the employee data.	Implement measures that automatically deal with changes to an employee's work role or workplace status and change the appropriate access rights accordingly.
P1.5	Ensuring limited duration of data storage	Employee data should only be stored and processed as long as it is necessary for the specified purpose.	Implement strict erasure rules that are executed when employees leave the company (A-P1.4).
P2.1	Legitimacy of processing personal data	Employees need to consent to the use of their data for access control. This consent can be part of their working contract or the like.	Ensure that consent forms are available and implement validity checks concerning the identity of the signee.
P3.1	Legitimacy of processing sensitive personal data	The human resource management system may contain sensitive personal data. The operator must ensure that this sensitive personal data is stored and processed only in that system and that access is limited strictly to human resource personnel. Employees need to explicitly consent to the processing of this sensitive personal data.	Inform employees that sensitive personal data might be handled in the human resource management system.
P4.1	Providing adequate information in cases of direct collection of data from the data subject	Ensure that employees are provided with information that describes the collected data. This data might be directly collected from the employees through the usage of access control cards or collected when he or she enrols as an employee.	Provision of adequate information, see P1.1.
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	- not applicable in this scenario - No data that is directly obtained from the employee, e.g. data from third parties, is processed in this scenario.	- not applicable in this scenario -
P5.1	Facilitating the provision of information about processed data and purpose	Employees should understand why data is collected purpose and the categories of collected data.	Provision of adequate information, see P1.1.
P5.2	Facilitating the rectification,	Employees should be allowed to rectify, erase or block their data. This right must be balanced against the	Provide employees with a contact address, form or the like that can

Privacy target code and name		Contextual explanation	Examples for how to reach this target
	erasure or blocking of data	legitimate use of access controls and human resource management systems.	be used to request rectification, erasure or blocking of their data.
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	- not applicable in this scenario - No employee data is handed over to a third party in this scenario.	- not applicable in this scenario -
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	- not applicable in this scenario - Direct marketing and data sharing of employees' personal data is not foreseen in this scenario. As part of a job contract and employment, the employee typically agrees to some data processing. Therefore, objection to this data processing is not possible.	- not applicable in this scenario -
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	- not applicable in this scenario - Employees should be able to object to being subject to automated decisions. No automated decisions are used in this scenario.	- not applicable in this scenario -
P7.1	Safeguarding confidentiality and security of processing	BSI's TG 03126-5 needs to be considered.	---
P8.1	Compliance with notification requirements	Before going live with the access control management system, the supervisory data protection authority needs to be notified about the related processing of personal data. The operator must also provide the results of the PIA to the supervisory authority six weeks before the launch.	The manufacturer should assign a person in his organisation to take care of these notifications. The assignee might need a project team to create the necessary documentation.

Table 48: Automotive-Access Control PIA – Definition of privacy targets

4.2.2.2 Step 3: Evaluation of protection demand categories

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.1	Ensuring fair and lawful processing through transparency	1	1	2	2	1	2

If the data processing activities related to the system landscape are not made transparent internally as well as externally to employees or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired, because most of the employees will not question how the access control system works. Employees might be used to similar access control procedures, and in most cases trust their employer. The brand is not affected.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired and employees ask for small changes to the access control system.
- employees' reputation can be seriously adversely affected (even without their knowledge) if access control data is used for a variety of purposes. Data might be used, for example, to create detailed profiles about their whereabouts on the manufacturer's premises, analyse work motivation, or analyse social relationships.
- employees' financial well-being can be seriously adversely affected if access control data is used to create detailed profiles about their whereabouts on the manufacturer's premises, analyse work motivation, or analyse social relationships. This data might also be used to inform layoff or promotion decisions.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 49: Automotive-Access Control PIA – Definition of protection demand categories for P1.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.2	Providing purpose specification and limitation	3	2	2	2	1	3

If the purpose and limitations of data processing are not specified, the RFID operator risks engaging in processing that is beyond the purposes for which data has been initially collected from data subjects. If such processing becomes known to the public, employees, journalists or the authorities, the parties that are involved may face the following consequences:

- the operator's reputation can suffer nation-wide impairment if detailed data about employees, especially sensitive personal data from the human resource management system, is used for purposes that were not specified or accessed by unauthorised parties. Employees can be considerably affected, and the press may question the company's internal ethics.
- the operator's financial loss can be considerable if its reputation is heavily impaired and resulting actions need to be taken. These actions may include investment in press activities, paying liabilities, etc.
- employees' reputation can be seriously adversely affected if detailed data about their whereabouts on the premises become known (potentially to unauthorised parties) and are used for purposes that were not specified and agreed upon. Such purposes can include analysis of employees' work motivation, potential health problems, relationships with others, etc. Also, sensitive data from the human resource system could – if abused – impact a person's social standing.
- employees' financial well-being can be seriously adversely affected if detailed data about their whereabouts on the premises or their sensitive personal data becomes known to unauthorised parties or is used for purposes that were not specified and agreed upon. Such purposes can include the use of data analysis to derive an employee's job motivation, which can in turn inform layoff or promotion decisions.
- employees' personal freedom cannot be endangered.

As one of the criteria is evaluated as high, the overall evaluation is “high – 3”.

Table 50: Automotive-Access Control PIA – Definition of protection demand categories for P1.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.3	Ensuring data avoidance and minimisation	1	1	2	2	1	2

If the principles of data avoidance and minimisation are not realised throughout the relevant applications and services, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because it is relatively unlikely that employees will find out that the operator collects more data than necessary if the operator sticks to the specified purpose and access control functionality.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there should be no need for costly adaptations (especially the implementation of minimisation measures) of the access control system.
- employees' reputation can be seriously adversely affected if more and/or more detailed data is collected over time than is necessary for the specified purpose and the access control functionality. For example, long term profiles allow for analysis of movement behaviour over time, which can be very revealing in terms of job motivation.
- employees' financial well-being can be seriously adversely affected if more and/or more detailed data is collected than is necessary for the specified purpose and the access control functionality. For example, long term profiles allow for analysis of movement behaviour over time, which can be very revealing in terms of job motivation. Such analysis again could inform layoff and promotion decisions.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 51: Automotive-Access Control PIA – Definition of protection demand categories for P1.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.4	Ensuring quality of data	2	2	1	1	1	2

If the quality (accuracy, up-to-dateness or completeness) of the personal data that is collected and processed is not ensured, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if employees get access – because of incorrect data – to facilities they are not allowed to enter or get access to confidential company assets. Such access can lead to critical security incidents.
- the operator's financial loss can be considerable if employees get access – because of incorrect data – to facilities they are not allowed to enter or get access to confidential company assets. As a result, critical security incidents might ensue.
- employees' reputation cannot be affected significantly.
- employees' financial well-being cannot be affected significantly.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 52: Automotive-Access Control PIA – Definition of protection demand categories for P1.4

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.5	Ensuring limited duration of data storage	1	1	2	2	1	2

If data is stored longer than necessary and no clear rules are implemented to limit data storage, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because it is relatively unlikely that employees will find out that the operator stores data longer than necessary if the operator sticks to the specified purpose and access control functionality.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there should be no need for costly adaptations (especially the implementation of data minimisation measures) of the access control system.
- employees' reputation can be seriously adversely affected if detailed data is stored longer than is necessary for the specified purpose and the access control functionality. In this case, data can accumulate, allowing the operator to trace employees' locations for a long period of time. Long term profiles allow for analysis of movement behaviour over time, which can be very revealing in terms of job motivation.
- employees' financial well-being can be seriously adversely affected if detailed data is stored longer than is necessary for the specified purpose and the access control functionality. In this case, data can accumulate, allowing the operator to trace employees' locations for a long period of time. Long term profiles allow, for analysis of movement behaviour over time, which can be very revealing in terms of job motivation. Such analysis again could inform layoff or promotion decisions.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 53: Automotive-Access Control PIA – Definition of protection demand categories for P1.5

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P2.1	Legitimacy of processing personal data	3	2	2	2	1	3

If the legitimacy of processing personal data is not ensured, e.g. via consent, the parties that are involved may face the following consequences:

- the operator's reputation can suffer nation-wide impairment because employees might feel betrayed and initiate lawsuits.
- the operator's financial loss can be considerable if its heavily impaired reputation results in costly image campaigns, adaptations of the access control system and costs for potential lawsuits.
- employees' reputation can be seriously adversely affected if personal data in the human resource system and movement information are used for illegitimate analysis. For example, personal data could be used to analyse work motivation, social relationships, and preferred whereabouts.
- employees' financial well-being can be seriously adversely affected if personal data in the human resource system and movement information are used for illegitimate analysis. For example, personal data could be used to analyse work motivation, social relationships, and preferred whereabouts. Such analysis again could inform layoff and promotion decisions.
- employees' personal freedom cannot be endangered.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 54: Automotive-Access Control PIA – Definition of protection demand categories for P2.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P3.1	Legitimacy of processing sensitive personal data	3	2	3	3	1	3

If the legitimacy of processing sensitive personal data is not ensured, e.g. via explicit consent, the parties that are involved may face the following consequences:

- the operator's reputation can suffer nation-wide impairment because employees might feel betrayed and initiate lawsuits.
- the operator's financial loss can be considerable if its heavily impaired reputation results in costly image campaigns, adaptations of the access control system and costs for potential lawsuits.
- employees' reputation can be devastatingly affected because detailed sensitive personal data might be collected, stored and processed that they are not aware of. For example, the system might store and process data on their health situation or information about their behaviour and performance on the job.
- employees' financial well-being can be devastatingly affected because detailed sensitive personal data might be collected, stored and processed that they are not aware of. For example, the system might store and process data on their health situation or information about their behaviour and performance on the job.
- employees' personal freedom cannot be endangered.

As most of the criteria are evaluated as high, the overall evaluation is “high – 3”.

Table 55: Automotive-Access Control PIA – Definition of protection demand categories for P3.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.1	Providing adequate information in cases of direct collection of data from the data subject	1	1	2	2	1	2

This privacy target is strongly related to P1.1, thus a similar analysis is used.

If the data processing activities related to the system landscape are not made transparent internally as well as externally to employees or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired, because most of the employees will not question how the access control system works. Employees might be used to similar access control procedures, and in most cases trust their employer. The brand is not affected.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired and employees ask for small changes to the access control system.
- employees' reputation can be seriously adversely affected (even without their knowledge) if access control data is used for a variety of purposes. Data might be used, for example, to create detailed profiles about their whereabouts on the manufacturer's premises, analyse work motivation, or analyse social relationships.
- employees' financial well-being can be seriously adversely affected if access control data is used to create detailed profiles about their whereabouts on the manufacturer's premises, analyse work motivation, or analyse social relationships. This data might also be used to inform layoff or promotion decisions.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 56: Automotive-Access Control PIA – Definition of protection demand categories for P4.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 57: Automotive-Access Control PIA – Definition of protection demand categories for P4.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.1	Facilitating the provision of information about processed data and purpose	1	1	1	1	1	1
If no information about processed data (i.e. in the form of data categories and items) and purpose is provided to the employees, the parties that are involved may face the following consequences: - the operator's reputation can be minimally impaired because few employees might enforce their legal rights vis-à-vis their employer to get insight into data stored about them. Most employees will probably trust their employer's benevolent use of data even if they do not get access to it. - the operator's financial loss can be acceptable if few employees enforce their legal rights to access their data. For those employees who do enforce their rights, the generation of detailed data processing reports might not be too costly. - employees' reputation cannot be affected significantly. - employees' financial well-being cannot be affected significantly. - employees' personal freedom cannot be endangered. As all of the criteria are evaluated as being low, the overall evaluation is “low – 1”.							

Table 58: Automotive-Access Control PIA – Definition of protection demand categories for P5.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.2	Facilitating the rectification, erasure or blocking of data	2	2	1	1	1	2

This privacy target is strongly related to P1.4, thus a similar analysis is used.

If employees are not enabled to rectify, erase or block their personal data, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if employees get access – because of incorrect data – to facilities they are not allowed to enter or get access to confidential company assets. Such access can lead to critical security incidents.
- the operator's financial loss can be considerable if employees get access – because of incorrect data – to facilities they are not allowed to enter or get access to confidential company assets. As a result, critical security incidents might ensue.
- employees' reputation cannot be affected significantly.
- employees' financial well-being cannot be affected significantly.
- employees' personal freedom cannot be endangered.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 59: Automotive-Access Control PIA – Definition of protection demand categories for P5.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	-	-	-	-	-	---

Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.

Table 60: Automotive-Access Control PIA – Definition of protection demand categories for P5.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 61: Automotive-Access Control PIA – Definition of protection demand categories for P6.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 62: Automotive-Access Control PIA – Definition of protection demand categories for P6.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P7.1	Safeguarding confidentiality and security of processing	-	-	-	-	-	---
BSI's TG 03126-5 needs to be considered.							

Table 63: Automotive-Access Control PIA – Definition of protection demand categories for P7.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Employee perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P8.1	Compliance with notification requirements	2	2	-	-	-	2
If the operator does not comply with the legally specified notification requirements, the parties that are involved may face the following consequences: - the operator's reputation can be considerably impaired because he might get into conflict with the supervisory data protection authority. These conflicts might be exposed to the public. - the operator's financial loss can be considerable if he is forced to pay fines, create the necessary documentation ad-hoc with the help of costly consultants and be subject to regular controls by the supervisory authority in the future. As all of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.							

Table 64: Automotive-Access Control PIA – Definition of protection demand categories for P8.1

4.2.2.3 Step 4: Identification of relevant threats

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			operator.		
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	y	
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	y	
		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.	y	
		T1.5	Existing information describing the service is not kept up-to-date.	y	
		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.	y	
	Lack of transparency – Missing or insufficient privacy statement	T1.7	No privacy statement is available.	y	
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	y	
		T1.9	The existing privacy statement does not provide a contact information to reach the RFID operator and does not provide contact details in case of questions or complaint.	y	
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	y	
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	n	Employee data is not handed over to third parties.
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	y	
	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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			collection process.		
		T1.14	No RFID emblem is displayed on the product and the product packaging.	n	Access control cards are the only “objects” that contain RFID tags.
	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.	y	
		T1.16	The data collection purpose is not documented in an adequate way.	y	
		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.	y	
	Collection and/or combination of data exceeding purpose	T1.18	Collected data is processed for other purposes than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	y	This threat is related to TT8 and TMS8 “Forbidden collection of additional information” ([BSI2010], p. 88 and 91).
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	y	
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	y	This threat is related to TT8 and TMS8 “Forbidden collection of additional information” ([BSI2010], p. 88 and 91).
		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.	y	This threat is related to TT8 and TMS8 “Forbidden collection of additional information” ([BSI2010], p. 88 and 91).
		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.	y	This threat is related to TMS9 “Not allowed linking of information” ([BSI2010], p. 91).
		T1.23	There are no measures in place that prevent the reading and tracking of the tagged item through unauthorised	y	This threat is related to TCM14 “Tracking by means of unauthorised

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			parties. The RFID tag has no read protection.		scanning by third parties" ([BSI2010], p. 85).
	Missing quality assurance of data	T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	y	
		T1.25	The identification of the data subject is not conducted thoroughly.	y	
		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.	y	
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	n	Employee accounts are not enriched by probabilistic algorithms.
	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.	y	
		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.	y	
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.	y	
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	y	
		T2.3	The relevant legal basis (e.g. consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.	y	
T3	Invalidation or non-existence of explicit consent	T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	y	
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	y	
		T3.3	The relevant legal basis (e.g. explicit	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			consent, field of employment law, vital interests, not-for-profit-body, published sensitive data, defence of legal claims, special legal basis) has been transgressed.		
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: - 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.	y	
		T4.2	The relevant information is not provided in an adequate form (e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	y	
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	y	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: - 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.	n	This threat belongs to P4.2, which was excluded from further consideration in step 2.
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	n	This threat belongs to P4.2, which was excluded from further consideration in step 2.

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		T4.6	The relevant information is not easily understandable so that it is possible that the data subject will not be able to understand that the operator obtained information on him or her from a third party.	n	This threat belongs to P4.2, which was excluded from further consideration in step 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.	y	
		T5.2	Access is possible but not to all relevant data, including: - 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.	y	
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	y	
		T5.4	Successful access as well as subsequent data disclosure is not logged.	y	
	Inability to rectify, erase or block individual data	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.	y	
		T5.6	Errors are not automatically rectified.	y	
		T5.7	There is no procedure that allows the erasure of individual data in back-up	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			data.		
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	y	
		T5.9	Successful rectification, erasure and blocking is not logged.	y	
	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.	n	This threat belongs to P5.3, which was excluded from further consideration in step 2.
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.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
		T6.3	The operator has not implemented any procedure that would allow the notification of relevant third parties in the case that a data subject has objected to the processing of his personal data.	n	This threat belongs to P6.1, which was excluded from further consideration in step 2.
	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.	n	This threat belongs to P6.2, which was excluded from further consideration in step 2.
T7	Refer to security-relevant threats that are defined in BSI's technical guidelines TG 03126-5.	T7.1	Refer to the description of security-relevant threats that are defined in BSI's technical guidelines TG 03126-5.	y	BSI's TG 03126-5 needs to be considered.
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.	y	
		T8.2	The operator does not provide all the	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			legally defined contents in his notification to the supervisory authority or the internal data protection officer.		
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	y	
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	y	

Table 65: Automotive-Access Control PIA – Identification of relevant threats

4.2.2.4 Step 5: Identification and recommendation of controls

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.1	C1.1 C1.4	SERVICE DESCRIPTION INFORMATION TIMELINESS	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.2	C1.2	INFORMATION ACCESSIBILITY	2 (P1.1)	The information describing the service is made accessible at the operator's physical facilities and online.
T1.3	C1.1	SERVICE DESCRIPTION	3 (max of P1.1 and P1.2)	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.
T1.4	C1.1 C1.3	SERVICE DESCRIPTION LANGUAGE / SEMANTICS OF INFORMATION	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. 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). The information describing the service is available in the most common languages and in languages that are potentially

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				specific to its target countries.
T1.5	C1.4	INFORMATION TIMELINESS	2 (P1.1)	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.6	C1.1	SERVICE DESCRIPTION	3 (max of P1.1 and P1.2)	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	INFORMATION ACCESSIBILITY		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.
T1.7	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.8	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.9	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.10	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.12	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.13	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.15	C1.7	PURPOSE SPECIFICATION	3	A purpose specification is available in two versions: a very detailed version for the involved employees of the operator

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
			(P1.2)	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.
T1.16	C1.7	PURPOSE SPECIFICATION	3 (max of P1.1 and P1.2)	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.
T1.17	C1.8	ENSURING LIMITED DATA PROCESSING	3 (P1.2)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level.
T1.18	C1.8 C1.9	ENSURING LIMITED DATA PROCESSING ENSURING PURPOSE RELATED PROCESSING	3 (max of P1.3 and TT8, TMS8 ([BSI2010], p. 160, 154, 164))	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. 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. Related safeguards from [BSI2010]: **MT1** "Introduction of interface tests and approval procedures": "Interface test: - Test of the interfaces of the terminal according to [ISO01], [ISO08a] or if applicable [BSI08b]. - Definition and usage of specific test specifications for the interfaces regarding the respective applications. - If applicable test of the interface that is provided in the offline or semi-offline scenario. Approval of components: - Approval of components within the terminal (e.g. key management, secure memory, applied SAMs, etc.) and components that are used in connection with the terminal (e.g. carrier medium) - If applicable approval of components that are used in case the terminal is used in an offline or semi-offline scenario. Certification:

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- Additional certification of the terminal (carrier medium) by and independent evaluation institution." (p. 126) **MT3** "Protection of reference information against retrieval, data errors and manipulation": "Reference information is processed by the terminal (if applicable in connection with the central information management system) in order to install, activate and deactivate applications and to administer the connected entitlements and application parameters. For example the following data is relevant: - (Application, File) identifiers - Keys (e.g. diversification keys, session keys, signature keys) Whitelists and Blacklists - Algorithms for evaluation Based on the applied applications different reference information, employee and usage data is relevant and is processed. Advanced protection: - Mechanisms for detecting data manipulation in the device, such as MAC-secured saving (provided this is possible from a performance point of view). - Data should only be transferred from management systems into the terminal after mutual authentication between the terminal and the respective instance with which a communication is performed. - Protected data transmission (i.e. secure messaging) to the carrier medium. - Application-specific separation of algorithms, reference data, usage data and keys. - Save the keys in an application-specific SAMs. - Save and execute cryptographic algorithms in an application-specific SAM. - Introduction of multi-tenant, application-specific access protection for the data in the terminal and administrative functions in accordance with the role model." (pp. 127-128) **MMS4** "Secure acquisition of data during personalisation and/or enrolment": "The acquisition of personal data (this includes also biometric data) is performed under the responsibility of the security manager and can only be conducted by an authorised instance. In general MMS6 shall be applied.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				The process for the acquisition is designed to capture only agreed personal data. The agreement is made with the working council or a comparable instance and the data protection official. The personal data is stored encrypted in the backend system e.g. the user account. Therefore the communication between the acquisition system and the backend system has to be encrypted by adequate mechanisms following [ALGK_BSI]. If furthermore data is written to the carrier medium this communication has to be ensured against unauthorised changes or manipulation by encryption (compare MMS2) and the data shall be stored protected by access control and if applicable encrypted (this applies in particular for biometric data). For the acquisition of biometric features the security manager shall be trained. The course of instruction shall include the processing in case a biometric feature is not available or cannot be captured. Advanced safeguards: - The communication between the terminal (if applicable with biometric acquisition unit) and computer system shall be encrypted." (p. 97) **MMS13** "Separation of applications": "Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105) **MMS15** "Satisfying the data minimalisation obligation": "Data minimalisation must be satisfied in accordance with the applicable legal regulations on privacy. Definition of relevant data: - It must be specified precisely which data needs to be available of the employee in order to implement and operate the system. It has to be paid attention to the fact that only minimal necessarily information shall be collected in accordance with the legal requirements. - Purpose-related definition of data content; data access and usage rights have to be specified and stored using the role model of the entire system. It is required to specify how long which kind of personal data is stored. Thereby,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				deadlines for deletion of data that is not needed any more shall be specified. - The collected data and the period of storage must be agreed with the working council or a comparable instance and the data protection official. Furthermore the following applies: - The employee is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 106)
T1.19	C1.9	ENSURING PURPOSE RELATED PROCESSING	2 (P1.3)	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.
T1.20	C1.10	ENSURING DATA MINIMISATION	3 (max of P1.3 and TT8, TMS8 ([BSI2010], p. 160, 154, 164))	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguards from [BSI2010]: **MT1** "Introduction of interface tests and approval procedures": "Interface test: - Test of the interfaces of the terminal according to [ISO01], [ISO08a] or if applicable [BSI08b]. - Definition and usage of specific test specifications for the interfaces regarding the respective applications. - If applicable test of the interface that is provided in the offline or semi-offline scenario. Approval of components: - Approval of components within the terminal (e.g. key management, secure memory, applied SAMs, etc.) and components that are used in connection with the terminal (e.g. carrier medium) - If applicable approval of components that are used in case the terminal is used in an offline or semi-offline scenario.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				Certification: - Additional certification of the terminal (carrier medium) by and independent evaluation institution." (p. 126) **MT3** "Protection of reference information against retrieval, data errors and manipulation": "Reference information is processed by the terminal (if applicable in connection with the central information management system) in order to install, activate and deactivate applications and to administer the connected entitlements and application parameters. For example the following data is relevant: - (Application, File) identifiers - Keys (e.g. diversification keys, session keys, signature keys) Whitelists and Blacklists - Algorithms for evaluation Based on the applied applications different reference information, employee and usage data is relevant and is processed. Advanced protection: - Mechanisms for detecting data manipulation in the device, such as MAC-secured saving (provided this is possible from a performance point of view). - Data should only be transferred from management systems into the terminal after mutual authentication between the terminal and the respective instance with which a communication is performed. - Protected data transmission (i.e. secure messaging) to the carrier medium. - Application-specific separation of algorithms, reference data, usage data and keys. - Save the keys in an application-specific SAMs. - Save and execute cryptographic algorithms in an application-specific SAM. - Introduction of multi-tenant, application-specific access protection for the data in the terminal and administrative functions in accordance with the role model." (pp. 127-128) **MMS4** "Secure acquisition of data during personalisation and/or enrolment": "The acquisition of personal data (this includes also biometric data) is performed under the responsibility of the security manager and can only be conducted by an authorised instance.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				In general MMS6 shall be applied. The process for the acquisition is designed to capture only agreed personal data. The agreement is made with the working council or a comparable instance and the data protection official. The personal data is stored encrypted in the backend system e.g. the user account. Therefore the communication between the acquisition system and the backend system has to be encrypted by adequate mechanisms following [ALGK_BSI]. If furthermore data is written to the carrier medium this communication has to be ensured against unauthorised changes or manipulation by encryption (compare MMS2) and the data shall be stored protected by access control and if applicable encrypted (this applies in particular for biometric data). For the acquisition of biometric features the security manager shall be trained. The course of instruction shall include the processing in case a biometric feature is not available or cannot be captured. Advanced safeguards: - The communication between the terminal (if applicable with biometric acquisition unit) and computer system shall be encrypted." (p. 97) **MMS13** "Separation of applications": "Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105) **MMS15** "Satisfying the data minimalisation obligation": "Data minimalisation must be satisfied in accordance with the applicable legal regulations on privacy. Definition of relevant data: - It must be specified precisely which data needs to be available of the employee in order to implement and operate the system. It has to be paid attention to the fact that only minimal necessarily information shall be collected in accordance with the legal requirements. - Purpose-related definition of data content; data access and usage rights have to be specified and stored using the role

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				model of the entire system. It is required to specify how long which kind of personal data is stored. Thereby, deadlines for deletion of data that is not needed any more shall be specified. - The collected data and the period of storage must be agreed with the working council or a comparable instance and the data protection official. Furthermore the following applies: - The employee is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 106)
T1.21	C1.10	ENSURING DATA MINIMISATION	3 (max of P1.3 and TT8, TMS8 ([BSI2010], p. 160, 154, 164))	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguards from [BSI2010]: **MT1** "Introduction of interface tests and approval procedures": "Interface test: - Test of the interfaces of the terminal according to [ISO01], [ISO08a] or if applicable [BSI08b]. - Definition and usage of specific test specifications for the interfaces regarding the respective applications. - If applicable test of the interface that is provided in the offline or semi-offline scenario. Approval of components: - Approval of components within the terminal (e.g. key management, secure memory, applied SAMs, etc.) and components that are used in connection with the terminal (e.g. carrier medium) - If applicable approval of components that are used in case the terminal is used in an offline or semi-offline scenario. Certification: - Additional certification of the terminal (carrier medium) by and independent evaluation institution." (p. 126)

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				MT3 “Protection of reference information against retrieval, data errors and manipulation”: “Reference information is processed by the terminal (if applicable in connection with the central information management system) in order to install, activate and deactivate applications and to administer the connected entitlements and application parameters. For example the following data is relevant: - (Application, File) identifiers - Keys (e.g. diversification keys, session keys, signature keys) Whitelists and Blacklists - Algorithms for evaluation Based on the applied applications different reference information, employee and usage data is relevant and is processed. Advanced protection: - Mechanisms for detecting data manipulation in the device, such as MAC-secured saving (provided this is possible from a performance point of view). - Data should only be transferred from management systems into the terminal after mutual authentication between the terminal and the respective instance with which a communication is performed. - Protected data transmission (i.e. secure messaging) to the carrier medium. - Application-specific separation of algorithms, reference data, usage data and keys. - Save the keys in an application-specific SAMs. - Save and execute cryptographic algorithms in an application-specific SAM. - Introduction of multi-tenant, application-specific access protection for the data in the terminal and administrative functions in accordance with the role model.” (pp. 127-128) **MMS4** “Secure acquisition of data during personalisation and/or enrolment”: “The acquisition of personal data (this includes also biometric data) is performed under the responsibility of the security manager and can only be conducted by an authorised instance. In general MMS6 shall be applied. The process for the acquisition is designed to capture only agreed personal data. The agreement is made with the working council or a comparable instance and the data protection

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				official. The personal data is stored encrypted in the backend system e.g. the user account. Therefore the communication between the acquisition system and the backend system has to be encrypted by adequate mechanisms following [ALGK_BSI]. If furthermore data is written to the carrier medium this communication has to be ensured against unauthorised changes or manipulation by encryption (compare MMS2) and the data shall be stored protected by access control and if applicable encrypted (this applies in particular for biometric data). For the acquisition of biometric features the security manager shall be trained. The course of instruction shall include the processing in case a biometric feature is not available or cannot be captured. Advanced safeguards: - The communication between the terminal (if applicable with biometric acquisition unit) and computer system shall be encrypted." (p. 97) **MMS13** "Separation of applications": "Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105) **MMS15** "Satisfying the data minimalisation obligation": "Data minimalisation must be satisfied in accordance with the applicable legal regulations on privacy. Definition of relevant data: - It must be specified precisely which data needs to be available of the employee in order to implement and operate the system. It has to be paid attention to the fact that only minimal necessarily information shall be collected in accordance with the legal requirements. - Purpose-related definition of data content; data access and usage rights have to be specified and stored using the role model of the entire system. It is required to specify how long which kind of personal data is stored. Thereby, deadlines for deletion of data that is not needed any more shall be specified.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- The collected data and the period of storage must be agreed with the working council or a comparable instance and the data protection official. Furthermore the following applies: - The employee is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 106)
T1.22	C1.8	ENSURING LIMITED DATA PROCESSING	3 (max of P1.3 and TMS9 ([BSI2010], p. 154, 164))	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. Related safeguard from [BSI2010]: **MMS13** "Separation of applications": "Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105)
T1.23	C1.11	ENSURING TAG PROTECTION	2 (max of P1.3 and TCM14 ([BSI2010], p. 182, 200, 223, 234))	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguards from [BSI2010]: **MCM4** "Protection of personal data against retrieval and manipulation": "Personal data (as described in § 3 of BDSG ("Bundesdatenschutzgesetz")) comprises - Information about a person (e. g. title, first name, surname, date of birth) - Biometric data (e.g. fingerprints) - Other personal usage data that is generated using the entitlement and sometimes stored in the application on the carrier medium. Protection of personal data - Access and write protection in accordance with MCM1 level 1.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- If only write protection is provided for the electronic chip, the personal data has to be protected with TDES, AES128 (preferably) or an open method of similar strength. The type and strength of the mechanism must be adjusted in line with future developments in accordance with [ALGK_BSI]. - Data is transmitted in encrypted form in accordance with MMS2 level 1, and will be stored in the electronic chip. Personal data and entitlements are protected using various keys. - Usage of diversification keys for the production of session keys. For eID documents security mechanisms such as e.g. [EAC10] that require certificates with respective entitlements are applied. Specific access protection for personal data - Access protection in accordance with MCM1 level 2. - Data is transmitted in secured form in accordance with MMS2 level 2, and will be stored in the electronic chip. Personal data and entitlements are protected using various keys. - The data may need to be protected against manipulation on the system side (e.g. using MAC). - Usage of diversification keys for the production of session keys. For eID documents security mechanisms such as e.g. [EAC10] that require certificates with respective entitlements are applied." (p. 112) **MCM6** "Separation of applications": "Separate storing and processing of data: - Applications are loaded in a secure environment which is under the control of the security manager. - If applications are provided by different application providers the entitlements have to be clearly separated from each other by a defined card structure. - In order to avoid coalition attacks, malfunction, and to ensure privacy the different card applications shall be provided with separate keys and entitlements for the according applications. - Diversification of keys for the provision of individual keys (e.g. session keys.) - Implementation of an application-specific access concept in

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				accordance with MCM1 level 2. Keys and rights are allocated in accordance with the role model of entities in the overall system. eID documents support separate applications such as e.g. eID and eSign applications." (p. 114) **MCM7** "Data minimisation": "Based on legal requirements (e.g. BDSG) the personal data that is used for the authentication processes in organisations has to be agreed with the working council or a comparable instance and the data protection official. Therefore, only data that is obligatory shall be included in the carrier medium." (p. 115)
T1.24	C1.12	ENSURING PERSONAL DATA QUALITY	2 (P1.4)	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.
T1.25	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2 (P1.4)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
T1.26	C1.14	ENSURING DATA ACCURACY	2 (P1.4)	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.
T1.28	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T1.29	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T2.1	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.2	C2.1	OBTAINING DATA	3	Legal personnel regularly checks if necessary consent is

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
		SUBJECT'S CONSENT	(P2.1)	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.
T2.3	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T3.1	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	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. 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.
T3.2	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	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. 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.
T3.3	C3.1	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	3 (P3.1)	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. 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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				awareness.
T4.1	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.2	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.3	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- 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.
T5.1	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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.
T5.2	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T5.3	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	1 (P5.1)	The data subject needs to identify or authenticate him or herself with his or her name and some security questions.
T5.4	C5.2	LOGGING ACCESS TO PERSONAL DATA	1 (P5.1)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T5.5	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.6	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.7	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2 (P5.2)	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 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.
T5.8	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2 (P5.2)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
T5.9	C5.2	LOGGING ACCESS TO	2	Data subjects' access to data, subsequent data disclosure,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
		PERSONAL DATA	(P5.2)	rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T7.1	C7.1	SECURITY CONTROLS	--- (P7.1)	See relevant controls from TG 03126-5.
T8.1	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.
T8.2	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.
T8.3	C8.2	PRIOR CHECKING	2 (P8.1)	It is ensured that the legally required checking of the RFID application is executed by expert personnel.
T8.4	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.

Table 66: Automotive-Access Control PIA – Identification and recommendation of controls

4.2.2.4.1 Consolidated view of identified controls

Control code and name		Highest overall category	Description
C1.1	SERVICE DESCRIPTION	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	INFORMATION ACCESSIBILITY	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-

Control code and name		Highest overall category	Description
			indexed and searchable.
C1.3	LANGUAGE / SEMANTICS OF INFORMATION	2	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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
C1.4	INFORMATION TIMELINESS	2	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
C1.5	PRIVACY STATEMENT	2	An extensive privacy statement that contains all required information in an easily understandable form is easily accessible, i.e. prominently linked on each web page of the operator.
C1.6	RFID EMBLEM	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.
C1.7	PURPOSE SPECIFICATION	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	ENSURING LIMITED DATA PROCESSING	3	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a fine-grained level. Related safeguard from [BSI2010]: **MMS13** “Separation of applications”: “Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system’s components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections.” (p. 105)
C1.9	ENSURING PURPOSE	3	It is regularly checked that collected data is used only for the

Control code and name		Highest overall category	Description
	RELATED PROCESSING		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. Related safeguards from [BSI2010]: **MT1** "Introduction of interface tests and approval procedures": "Interface test: - Test of the interfaces of the terminal according to [ISO01], [ISO08a] or if applicable [BSI08b]. - Definition and usage of specific test specifications for the interfaces regarding the respective applications. - If applicable test of the interface that is provided in the offline or semi-offline scenario. Approval of components: - Approval of components within the terminal (e.g. key management, secure memory, applied SAMs, etc.) and components that are used in connection with the terminal (e.g. carrier medium) - If applicable approval of components that are used in case the terminal is used in an offline or semi-offline scenario. Certification: - Additional certification of the terminal (carrier medium) by and independent evaluation institution." (p. 126) **MT3** "Protection of reference information against retrieval, data errors and manipulation": "Reference information is processed by the terminal (if applicable in connection with the central information management system) in order to install, activate and deactivate applications and to administer the connected entitlements and application parameters. For example the following data is relevant: - (Application, File) identifiers - Keys (e.g. diversification keys, session keys, signature keys) Whitelists and Blacklists - Algorithms for evaluation Based on the applied applications different reference information, employee and usage data is relevant and is processed. Advanced protection: - Mechanisms for detecting data manipulation in the device, such as MAC-secured saving (provided this is possible

Control code and name		Highest overall category	Description
			from a performance point of view). - Data should only be transferred from management systems into the terminal after mutual authentication between the terminal and the respective instance with which a communication is performed. - Protected data transmission (i.e. secure messaging) to the carrier medium. - Application-specific separation of algorithms, reference data, usage data and keys. - Save the keys in an application-specific SAMs. - Save and execute cryptographic algorithms in an application-specific SAM. - Introduction of multi-tenant, application-specific access protection for the data in the terminal and administrative functions in accordance with the role model." (pp. 127-128) **MMS4** "Secure acquisition of data during personalisation and/or enrolment": "The acquisition of personal data (this includes also biometric data) is performed under the responsibility of the security manager and can only be conducted by an authorised instance. In general MMS6 shall be applied. The process for the acquisition is designed to capture only agreed personal data. The agreement is made with the working council or a comparable instance and the data protection official. The personal data is stored encrypted in the backend system e.g. the user account. Therefore the communication between the acquisition system and the backend system has to be encrypted by adequate mechanisms following [ALGK_BSI]. If furthermore data is written to the carrier medium this communication has to be ensured against unauthorised changes or manipulation by encryption (compare MMS2) and the data shall be stored protected by access control and if applicable encrypted (this applies in particular for biometric data). For the acquisition of biometric features the security manager shall be trained. The course of instruction shall include the processing in case a biometric feature is not available or cannot be captured. Advanced safeguards: - The communication between the terminal (if applicable with biometric acquisition unit) and computer system shall be encrypted." (p. 97) **MMS13** "Separation of applications": "Separate storing and processing of data:

Control code and name		Highest overall category	Description
			- In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105) **MMS15** "Satisfying the data minimalisation obligation": "Data minimalisation must be satisfied in accordance with the applicable legal regulations on privacy. Definition of relevant data: - It must be specified precisely which data needs to be available of the employee in order to implement and operate the system. It has to be paid attention to the fact that only minimal necessarily information shall be collected in accordance with the legal requirements. - Purpose-related definition of data content; data access and usage rights have to be specified and stored using the role model of the entire system. It is required to specify how long which kind of personal data is stored. Thereby, deadlines for deletion of data that is not needed any more shall be specified. - The collected data and the period of storage must be agreed with the working council or a comparable instance and the data protection official. Furthermore the following applies: - The employee is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 106)
C1.10	ENSURING DATA MINIMISATION	3	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. Additionally, there are technical procedures in place, which ensure data minimisation (for technical control examples, see Table 6, in particular automated enforcement of deletion policies, implementation of anonymisation, pseudonymisation and obfuscation) during processing of data. Related safeguards from [BSI2010]: **MT1** "Introduction of interface tests and approval procedures": "Interface test:

Control code and name		Highest overall category	Description
			- Test of the interfaces of the terminal according to [ISO01], [ISO08a] or if applicable [BSI08b]. - Definition and usage of specific test specifications for the interfaces regarding the respective applications. - If applicable test of the interface that is provided in the offline or semi-offline scenario. Approval of components: - Approval of components within the terminal (e.g. key management, secure memory, applied SAMs, etc.) and components that are used in connection with the terminal (e.g. carrier medium) - If applicable approval of components that are used in case the terminal is used in an offline or semi-offline scenario. Certification: - Additional certification of the terminal (carrier medium) by and independent evaluation institution." (p. 126) **MT3** "Protection of reference information against retrieval, data errors and manipulation": "Reference information is processed by the terminal (if applicable in connection with the central information management system) in order to install, activate and deactivate applications and to administer the connected entitlements and application parameters. For example the following data is relevant: - (Application, File) identifiers - Keys (e.g. diversification keys, session keys, signature keys) Whitelists and Blacklists - Algorithms for evaluation Based on the applied applications different reference information, employee and usage data is relevant and is processed. Advanced protection: - Mechanisms for detecting data manipulation in the device, such as MAC-secured saving (provided this is possible from a performance point of view). - Data should only be transferred from management systems into the terminal after mutual authentication between the terminal and the respective instance with which a communication is performed. - Protected data transmission (i.e. secure messaging) to the carrier medium. - Application-specific separation of algorithms, reference data, usage data and keys.

Control code and name		Highest overall category	Description
			- Save the keys in an application-specific SAMs. - Save and execute cryptographic algorithms in an application-specific SAM. - Introduction of multi-tenant, application-specific access protection for the data in the terminal and administrative functions in accordance with the role model." (pp. 127-128) **MMS4** "Secure acquisition of data during personalisation and/or enrolment": "The acquisition of personal data (this includes also biometric data) is performed under the responsibility of the security manager and can only be conducted by an authorised instance. In general MMS6 shall be applied. The process for the acquisition is designed to capture only agreed personal data. The agreement is made with the working council or a comparable instance and the data protection official. The personal data is stored encrypted in the backend system e.g. the user account. Therefore the communication between the acquisition system and the backend system has to be encrypted by adequate mechanisms following [ALGK_BSI]. If furthermore data is written to the carrier medium this communication has to be ensured against unauthorised changes or manipulation by encryption (compare MMS2) and the data shall be stored protected by access control and if applicable encrypted (this applies in particular for biometric data). For the acquisition of biometric features the security manager shall be trained. The course of instruction shall include the processing in case a biometric feature is not available or cannot be captured. Advanced safeguards: - The communication between the terminal (if applicable with biometric acquisition unit) and computer system shall be encrypted." (p. 97) **MMS13** "Separation of applications": "Separate storing and processing of data: - In order to prevent the malfunction and misuse of key materials and data, the applications must be separated in all of the system's components. Furthermore the application might belong to different application providers. - Defined access to applications is established for authorised instances. - Separation of card applications and the keys (carrier media, SAM) are described in the respective sections." (p. 105) **MMS15** "Satisfying the data minimalisation obligation":

Control code and name		Highest overall category	Description
			"Data minimalisation must be satisfied in accordance with the applicable legal regulations on privacy. Definition of relevant data: - It must be specified precisely which data needs to be available of the employee in order to implement and operate the system. It has to be paid attention to the fact that only minimal necessarily information shall be collected in accordance with the legal requirements. - Purpose-related definition of data content; data access and usage rights have to be specified and stored using the role model of the entire system. It is required to specify how long which kind of personal data is stored. Thereby, deadlines for deletion of data that is not needed any more shall be specified. - The collected data and the period of storage must be agreed with the working council or a comparable instance and the data protection official. Furthermore the following applies: - The employee is informed about the purpose-related acquisition, storage and use of personal data and data that can be related to particular people." (p. 106)
C1.11	ENSURING TAG PROTECTION	2	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject. Related safeguards from [BSI2010]: **MCM4** "Protection of personal data against retrieval and manipulation": "Personal data (as described in § 3 of BDSG ("Bundesdatenschutzgesetz")) comprises - Information about a person (e. g. title, first name, surname, date of birth) - Biometric data (e.g. fingerprints) - Other personal usage data that is generated using the entitlement and sometimes stored in the application on the carrier medium. Protection of personal data - Access and write protection in accordance with MCM1 level 1. - If only write protection is provided for the electronic chip, the personal data has to be protected with TDES, AES128 (preferably) or an open method of similar strength. The type and strength of the mechanism must be adjusted in line with future developments in accordance with [ALGK_BSI].

Control code and name		Highest overall category	Description
			- Data is transmitted in encrypted form in accordance with MMS2 level 1, and will be stored in the electronic chip. Personal data and entitlements are protected using various keys. - Usage of diversification keys for the production of session keys. For eID documents security mechanisms such as e.g. [EAC10] that require certificates with respective entitlements are applied. Specific access protection for personal data - Access protection in accordance with MCM1 level 2. - Data is transmitted in secured form in accordance with MMS2 level 2, and will be stored in the electronic chip. Personal data and entitlements are protected using various keys. - The data may need to be protected against manipulation on the system side (e.g. using MAC). - Usage of diversification keys for the production of session keys. For eID documents security mechanisms such as e.g. [EAC10] that require certificates with respective entitlements are applied." (p. 112) **MCM6** "Separation of applications": "Separate storing and processing of data: - Applications are loaded in a secure environment which is under the control of the security manager. - If applications are provided by different application providers the entitlements have to be clearly separated from each other by a defined card structure. - In order to avoid coalition attacks, malfunction, and to ensure privacy the different card applications shall be provided with separate keys and entitlements for the according applications. - Diversification of keys for the provision of individual keys (e.g. session keys.) - Implementation of an application-specific access concept in accordance with MCM1 level 2. Keys and rights are allocated in accordance with the role model of entities in the overall system. eID documents support separate applications such as e.g. eID and eSign applications." (p. 114) **MCM7** "Data minimisation": "Based on legal requirements (e.g. BDSG) the personal data that is used for the authentication processes in organisations

Control code and name		Highest overall category	Description
			has to be agreed with the working council or a comparable instance and the data protection official. Therefore, only data that is obligatory shall be included in the carrier medium." (p. 115)
C1.12	ENSURING PERSONAL DATA QUALITY	2	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.
C1.13	ENSURING DATA SUBJECT AUTHENTICATION	2	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
C1.14	ENSURING DATA ACCURACY	2	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	ENABLING DATA DELETION	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.
C2.1	OBTAINING DATA SUBJECT'S CONSENT	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	OBTAINING DATA SUBJECT'S EXPLICIT CONSENT	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	PROVIDING INFORMATION PROCESSING INFORMATION	2	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

Control code and name		Highest overall category	Description
			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.
C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1	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: - 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. 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.
C5.2	LOGGING ACCESS TO PERSONAL DATA	2	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	2	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 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.
C7.1	SECURITY CONTROLS	---	See relevant controls from TG 03126-5.

Control code and name		Highest overall category	Description
C8.1	NOTIFICATION OF AUTHORITY	2	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 weeks prior to the RFID application's launch.
C8.2	PRIOR CHECKING	2	It is ensured that the legally required checking of the RFID application is executed by expert personnel.

Table 67: Automotive-Access Control PIA – Consolidated view of identified controls

4.2.2.5 Step 6: Documentation of residual risks

For technical or business reasons it is not always possible to eliminate threats completely by applying controls. Some residual risks remain. These residual risks should be documented in this step. It is recommended to provide a comprehensive description and an evaluation (low, medium, high) for each residual risk.

4.2.3 The usage of RFID tags for manufacturing, delivery and defect management purposes

4.2.3.1 Step 2: Definition of privacy targets

In this step, stakeholders should discuss the privacy targets that are described in the PIA Framework and the concrete instances of those privacy targets as described in the PIA guideline. By discussing the targets and their instances, stakeholders can clarify what the targets mean in the context of the specific RFID application and corresponding business cases.

Privacy target code and name		Contextual explanation	**Examples** for how to reach this target
P1.1	Ensuring fair and lawful processing through transparency	The customers need to know that RFID technology is integrated into their cars and how this technology works. The information should be prepared in an understandable and easily accessible way.	Provide informational material with each car when it is handed over to a customer and duplicate this information on web pages. Train car dealer personnel and other personnel who have customer contact.
P1.2	Providing purpose specification and limitation	The operator must specify why the customer data in the car dealer management system is collected and stored. For example, customer data might be collected for defect management purposes. The car body tag is used to identify the car during its entire lifetime. Module tags are used for plagiarism	Provide customers with clear internal and external purpose specifications so that access rights can be handled accordingly. Customers should be well informed about what their personal data is used for.

Privacy target code and name		**Contextual explanation**	**Examples** for how to reach this target
		and recall cases.	
P1.3	Ensuring data avoidance and minimisation	When designing and implementing the distribution- and car dealer management systems, the operator must ensure that only necessary customer data is collected and processed. In this context, necessary means needed for the fulfilment of the specified purpose.	Collect only customer data that is needed to enable defect management and offer other car dealer services.
P1.4	Ensuring quality of data	Customer data that is stored in the distribution- and car dealer management systems needs to be regularly checked to ensure that it is correct and up-to-date. The seamless functioning of the defect management system heavily depends on the accuracy of the customer data.	Implement measures that regularly check the accuracy of customer data.
P1.5	Ensuring limited duration of data storage	Customer data should only be stored and processed as long as is necessary for the specified purpose.	If possible, regularly erase some of the customer data after a specified period of time.
P2.1	Legitimacy of processing personal data	When customers buy a car or use other car dealer services, they need to explicitly agree with the use of their personal data for defect management and/or other car dealer services.	Ensure that consent forms are available and implement validity checks concerning the identity of the signee.
P3.1	Legitimacy of processing sensitive personal data	- not applicable in this scenario - No sensitive personal data is collected or processed in this scenario.	- not applicable in this scenario -
P4.1	Providing adequate information in cases of direct collection of data from the data subject	As data is directly collected from customers when they acquire a car, the operator must ensure that customers receive information that describes what data is collected.	Provision of adequate information, see P1.1.
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	Several parties are involved in the defect management and recall procedure; these parties include the manufacturer and several car dealers. Thus, data that is not directly obtained from the customer is processed in some cases.	Provision of adequate information, see P4.1.
P5.1	Facilitating the provision of information about processed data and purpose	Customers must be informed about the purpose of the data collection as well as the collected data categories.	Provision of adequate information, see P1.1.
P5.2	Facilitating the	Customers should be allowed to rectify, erase or block	Provide a contact address, form or

Privacy target code and name		**Contextual explanation**	**Examples** for how to reach this target
	rectification, erasure or blocking of data	their data. Car dealer management systems need to be considered.	the like that customers can use to request rectification, erasure or blocking of their data.
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	Because customer data is exchanged between the manufacturer and car dealers, a notification mechanism is needed.	Both, the manufacturer and the car dealer, need to implement a mechanism that notifies third parties about changes in customer data.
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	Customers must be able to object to the processing of their data for direct marketing purposes or disclosure to third parties. Customer data is not used for the purpose of direct marketing in this scenario. But customer data is disclosed to third parties, thus customers must be able to object to such a disclosure.	Both, the manufacturer and the car dealer, need to offer a procedure or a mechanism that allows customers to object to the disclosure of their data to third parties.
P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	- not applicable in this scenario - The operator must allow customers to object to being subject to automated decisions. No automated decisions are used in this scenario.	- not applicable in this scenario -
P7.1	Safeguarding confidentiality and security of processing	BSI's TG 03126 needs to be considered.	---
P8.1	Compliance with notification requirements	Before going live with the defect and car dealer management systems, The operator must notify the supervisory data protection authority about the related processing of personal data. The operator must also provide the results of the PIA to the supervisory authority six weeks before the launch.	Both, the manufacturer and the car dealer, should assign a person in their organisation to take care of these notifications. The assignee might need a project team to create the necessary documentation.

Table 68: Automotive-Manufacturing PIA – Definition of privacy targets

4.2.3.2 Step 3: Evaluation of protection demand categories

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.1	Ensuring fair and lawful processing through transparency	2	2	1	1	2	2

If the data processing activities related to the system landscape are not made transparent internally as well as externally to customers or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because details about how the car body tag and module tags work are difficult to understand. No similar applications already exist. Customers might therefore feel betrayed and go public if they only understand the details later on.
- the operator's financial loss can be considerable if its reputation is considerably impaired. This damage might cause customers to stop buying the manufacturer's cars and require costly image campaigns to restore customers' faith.
- customers' reputation cannot be affected significantly.
- customers' financial well-being cannot be affected significantly.
- customers' personal freedom cannot be endangered. If the customers have known and understood the workings of the RFID technology in advance, they could have decided against buying one of the manufacturer's cars.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 69: Automotive-Manufacturing PIA – Definition of protection demand categories for P1.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.2	Providing purpose specification and limitation	2	2	2	2	1	2

If the purpose and limitations of data processing are not specified, the RFID operator risks engaging in processing that is beyond the purposes for which data has been initially collected from data subjects. If such processing becomes known to the public, customers, journalists or the authorities, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired if detailed data about customers' driving and repair history is used for purposes that were not specified and are accessed by unauthorised parties. Customers might be affected negatively.
- the operator's financial loss can be considerable if its reputation is considerably impaired. This damage might lead customers to stop buying the manufacturer's cars and require costly image campaigns to restore the customers' faith.
- customers' reputation can be seriously adversely affected if their driving and repair history becomes known to unauthorised parties and is used for purposes that were not specified and agreed upon.
- customers' financial well-being can be seriously adversely affected if their driving and repair history becomes known to unauthorised parties (i.e. insurance companies) and is used for purposes that were not specified and agreed upon. For example, customers' driving and repair history might lead to disadvantageous future contracts.
- customers' personal freedom cannot be endangered.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 70: Automotive-Manufacturing PIA – Definition of protection demand categories for P1.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.3	Ensuring data avoidance and minimisation	1	1	1	2	2	2

If the principles of data avoidance and minimisation are not realised throughout the relevant applications and services, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired if the operator sticks to the specified purpose and defect management functionality. It is not very likely that customers will find out that the operator collects more data than necessary.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there is no need for costly adaptations (especially the implementation of data minimisation measures) of the defect management procedure and systems.
- customers' reputation can be adversely affected if more and/or more detailed data is collected that allows others to make conclusions about their driving style, maintenance habits, etc.
- customers' financial well-being can be seriously adversely affected if more and/or more detailed data is collected that allows others to make conclusions about their driving style, maintenance habits, etc. These insights might be used to target later offerings to customers.
- customers' personal freedom could be endangered if more and/or more detailed data is collected from their cars and they cannot prevent this collection.

As two of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 71: Automotive-Manufacturing PIA – Definition of protection demand categories for P1.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.4	Ensuring quality of data	2	2	1	2	3	3

If the quality (accuracy, up-to-dateness or completeness) of the personal data that is collected and processed is not ensured, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because the seamless and effective functioning of the defect management system, including recall procedures, depends heavily on the accuracy of data.
- the operator's financial loss can be considerable if its reputation is considerably damaged and a costly “manual” recall needs to be conducted.
- customers' reputation cannot be affected significantly.
- customers' financial well-being can be seriously adversely affected if they are wrongly included or left out of a recall procedure and customers suffer higher repair costs later on. Also, faulty information about customers' driving style and maintenance history may lead to higher insurance costs or lower returns on car sales.
- customers' personal freedom could be seriously endangered if they are wrongly left out of a recall procedure and the defect module causes a serious accident.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 72: Automotive-Manufacturing PIA – Definition of protection demand categories for P1.4

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P1.5	Ensuring limited duration of data storage	1	1	2	2	2	2

If data is stored longer than necessary and no clear rules are implemented to limit data storage, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired if the operator sticks to the specified purpose and defect management functionality. It is not very likely that customers will find out that the operator stores data longer than necessary.
- the operator's financial loss can be acceptable if its reputation is only minimally impaired. As a result, there should be no need for costly adaptations (especially the implementation of data minimisation measures) of the defect management procedure and the involved systems.
- customers' reputation can be seriously adversely affected if detailed data is stored longer than necessary for the specified purpose and the defect management functionality. In this case, the data accumulates and allows the operator to collect customers' driving and repair history over a long period of time.
- customers' financial well-being can be seriously adversely affected if detailed data is stored that reflects customers' driving and repair history over a long period of time. This data might influence future insurance terms, car offerings or take-back of used cars.
- customers' personal freedom could be endangered if more and/or more detailed data is collected and stored for long periods of time from their cars and they cannot prevent this collection.

As most of the criteria are evaluated as medium, the overall evaluation is “medium – 2”.

Table 73: Automotive-Manufacturing PIA – Definition of protection demand categories for P1.5

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P2.1	Legitimacy of processing personal data	3	2	1	2	1	3

If the legitimacy of processing personal data is not ensured, e.g. via consent, the parties that are involved may face the following consequences:

- the operator's reputation can suffer nation-wide impairment because customers might feel betrayed and initiate lawsuits.
- the operator's financial loss can be considerable if its reputation is heavily impaired and results in costly image campaigns, adaptations of the defect management procedures and systems and costs for potential lawsuits.
- customers' reputation can be adversely affected if detailed personal data (such as driving style, maintenance patterns) are collected, stored and processed that they are not aware of.
- customers' financial well-being can be seriously adversely affected if detailed personal data is collected, stored and processed that they are not aware of. This data may be used by insurance companies or car dealers later to determine disadvantageous terms and conditions.
- customers' personal freedom cannot be endangered.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 74: Automotive-Manufacturing PIA – Definition of protection demand categories for P2.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P3.1	Legitimacy of processing sensitive personal data	-	-	-	-	-	---

Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.

Table 75: Automotive-Manufacturing PIA – Definition of protection demand categories for P3.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.1	Providing adequate information in cases of direct collection of data from the data subject	2	2	1	1	2	2

This privacy target is strongly related to P1.1, thus a similar analysis is used.

If the data processing activities related to the system landscape are not made transparent internally as well as externally to customers or other requesting parties, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because details about how the car body tag and module tags work are difficult to understand. No similar applications already exist. Customers might therefore feel betrayed and go public if they only understand the details later on.
- the operator's financial loss can be considerable if its reputation is considerably impaired. This damage might cause customers to stop buying the manufacturer's cars and require costly image campaigns to restore customers' faith.
- customers' reputation cannot be affected significantly.
- customers' financial well-being cannot be affected significantly.
- customers' personal freedom cannot be endangered. If the customers have known and understood the workings of the RFID technology in advance, they could have decided against buying one of the manufacturer's cars.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 76: Automotive-Manufacturing PIA – Definition of protection demand categories for P4.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P4.2	Providing adequate information where the data has not been obtained directly from the data subject	2	2	1	1	2	2

The dealer and the car manufacturer are exchanging defect management information which could contain personal information.

If no adequate information is provided to customers about data that has not been obtained directly from them but through data exchanges of involved parties, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because details about how car body tag and module tags work, as well as related defect management procedures (that include the exchange of personal data), are difficult to understand for a customer. No similar applications exist. As a result, customers might feel betrayed if they find out that such data is exchanged between their dealer and the manufacturer.
- the operator's financial loss can be considerable if its reputation is considerably impaired. This damage might lead customers to stop buying the manufacturer's cars and require costly image campaigns to restore the customers' faith.
- customers' reputation can be adversely affected if they did not know in advance what kind of data is collected and processed, e.g. when visiting a car dealer.
- customers' financial well-being can be adversely affected if they did not know in advance what kind of data is collected and processed, e.g. when visiting a car dealer.
- customers' personal freedom could be endangered. If they had known and understood the workings of the RFID technology in advance, they could have decided against buying one of the manufacturer's cars.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 77: Automotive-Manufacturing PIA – Definition of protection demand categories for P4.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.1	Facilitating the provision of information about processed data and purpose	1	1	1	1	1	1

If no information about processed data (i.e. in the form of data categories and items) and purpose is provided to the customers, the parties that are involved may face the following consequences:

- the operator's reputation can be minimally impaired because only a few customers might enforce their legal rights and force the operator to provide a detailed overview of their processed data.
- the operator's financial loss can be acceptable because the generation of such detailed data processing reports for some customers might not be too costly.
- customers' reputation cannot be affected significantly.
- customers' financial well-being cannot be affected significantly.
- customers' personal freedom cannot be endangered.

As all of the criteria are evaluated as being low, the overall evaluation is “low – 1”.

Table 78: Automotive-Manufacturing PIA – Definition of protection demand categories for P5.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.2	Facilitating the rectification, erasure or blocking of data	2	2	1	2	3	3

This privacy target is strongly related to P1.4, thus a similar analysis is used.

If customers are not enabled to rectify, erase or block their personal data, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because the seamless and effective functioning of the defect management system, including recall procedures, depends heavily on the accuracy of data.
- the operator's financial loss can be considerable if its reputation is considerably damaged and a costly “manual” recall needs to be conducted.
- customers' reputation cannot be affected significantly.
- customers' financial well-being can be seriously adversely affected if they are wrongly included or left out of a recall procedure and customers suffer higher repair costs later on. Also, faulty information about customers' driving style and maintenance history may lead to higher insurance costs or lower returns on car sales.
- customers' personal freedom could be seriously endangered if they are wrongly left out of a recall procedure and the defect module causes a serious accident.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 79: Automotive-Manufacturing PIA – Definition of protection demand categories for P5.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	2	2	1	2	3	3

This privacy target is strongly related to P5.2, thus a similar analysis is used.

If involved third parties are not notified about rectification, erasure and blocking of data, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because the seamless and effective functioning of the defect management system, including recall procedures, depends heavily on the accuracy of data.
- the operator's financial loss can be considerable if its reputation is considerably damaged and a costly “manual” recall needs to be conducted.
- customers' reputation cannot be affected significantly.
- customers' financial well-being can be seriously adversely affected if they are wrongly included or left out of a recall procedure and customers suffer higher repair costs later on. Also, faulty information about customers' driving style and maintenance history may lead to higher insurance costs or lower returns on car sales.
- customers' personal freedom could be seriously endangered if they are wrongly left out of a recall procedure and the defect module causes a serious accident.

As one of the criteria is evaluated as being high, the overall evaluation is “high – 3”.

Table 80: Automotive-Manufacturing PIA – Definition of protection demand categories for P5.3

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	2	2	2	2	1	2

If customers are not enabled to object to the processing of their personal data (e.g. for direct marketing purposes or disclosure to third parties), the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because if detailed data about customers' driving and repair history is used by an unknown third party, customers might suffer negative consequences.
- the operator's financial loss can be considerable if its reputation is considerably impaired. Such damage might lead customers to stop buying the manufacturer's cars and require costly image campaigns to restore the customers' faith.
- customers' reputation can be seriously adversely affected if their driving and repair history becomes known to unknown and thus unauthorised third parties. These parties might use the information for purposes that were not specified and agreed upon.
- customers' financial well-being can be seriously adversely affected if their driving and repair history becomes known to unknown and thus unauthorised third parties. These parties might use the information for purposes that were not specified and agreed upon.
- customers' personal freedom cannot be endangered.

As most of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 81: Automotive-Manufacturing PIA – Definition of protection demand categories for P6.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P6.2	Facilitating the objection to being subject to decisions which are solely based on automated processing of data	-	-	-	-	-	---
Step 2 lead to the conclusion not to consider this privacy target throughout the following steps of the PIA.							

Table 82: Automotive-Manufacturing PIA – Definition of protection demand categories for P6.2

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P7.1	Safeguarding confidentiality and security of processing	-	-	-	-	-	---
BSI's TG 03126 needs to be considered.							

Table 83: Automotive-Manufacturing PIA – Definition of protection demand categories for P7.1

Privacy target code and name		Criteria for the classification of protection demand categories					Overall category
		Operator perspective		Customer perspective			
		Impact on Reputation and Brand Value	Financial loss	Social standing, reputation	Financial well-being	Personal freedom	
P8.1	Compliance with notification requirements	2	2	-	-	-	2

If the operator does not comply with the legally specified notification requirements, the parties that are involved may face the following consequences:

- the operator's reputation can be considerably impaired because he might get into conflict with the supervisory data protection authority. These conflicts might be exposed to the public.
- the operator's financial loss can be considerable if he is forced to pay fines, create the necessary documentation ad-hoc with the help of costly consultants and be subject to regular controls by the supervisory authority in the future.

As all of the criteria are evaluated as being medium, the overall evaluation is “medium – 2”.

Table 84: Automotive-Manufacturing PIA – Definition of protection demand categories for P8.1

4.2.3.3 Step 4: Identification of relevant threats

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
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.	y	
		T1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable.	y	
		T1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	y	
		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.	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		T1.5	Existing information describing the service is not kept up-to-date.	y	
		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.	y	
	Lack of transparency – Missing or insufficient privacy statement	T1.7	No privacy statement is available.	y	
		T1.8	Existing privacy statement does not explain sufficiently how data subject's data is processed.	y	
		T1.9	The existing privacy statement does not provide a contact information to reach the RFID Operator and does not provide contact details in case of questions or complaint.	y	
		T1.10	The existing privacy statement is difficult to access; i.e. difficult to read, difficult to find, etc.	y	
		T1.11	The existing privacy statement does not contain information about relevant third parties that also receive the data subject's data.	y	
		T1.12	The existing privacy statement is not available in the various languages in which it will most probably be read.	y	
	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.	y	
		T1.14	No RFID emblem is displayed on the product and the product packaging.	y	
	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.	y	
		T1.16	The data collection purpose is not documented in an adequate way.	y	
		T1.17	Data that is stored and processed only for a specific purpose is not marked and / or managed accordingly; e.g. with	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			corresponding access rights.		
	Collection and/or combination of data exceeding purpose	T1.18	Collected data is processed for other purposes than the purpose it was originally obtained for. These different purposes are not compatible with the original purpose.	y	
		T1.19	Processing of data is not logged, thus misuse or processing for another purpose cannot be detected.	y	
		T1.20	The data subject is required to provide personal data that is not relevant for the specified purpose of the service.	y	
		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.	y	
		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.	y	
		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.	y	
	Missing quality assurance of data	T1.24	Data collection tools / forms are not sufficiently checked for completeness and correctness.	y	
		T1.25	The identification of the data subject is not conducted thoroughly.	y	
		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.	y	
		T1.27	Personally identifiable data-subject profiles are enriched by probabilistic algorithms that lead to false judgements about a data subject.	n	Customer accounts are not enriched by probabilistic algorithms.

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
	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.	y	
		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.	y	
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.	y	
		T2.2	Consent has been obtained based on an offer of advantage or threat of disadvantage.	y	
		T2.3	The relevant legal basis (e.g. consent, contract, legal obligation, vital interests, public task, balancing interests) has been transgressed.	y	
T3	Invalidation or non-existence of explicit consent	T3.1	Explicit consent has not been obtained or has been obtained on the basis of incomplete or incorrect information.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
		T3.2	Explicit consent has been obtained based on an offer of advantage or threat of disadvantage.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
		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.	n	This threat belongs to P3.1, which was excluded from further consideration in step 2.
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: - 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	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
			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.		
		T4.2	The relevant information is not provided in an adequate form (e.g. explicitly in the data collection questionnaire, small pop-up box that is easily clicked away).	y	
		T4.3	The relevant information is not easily accessible but hidden (e.g. small print in a legal section).	y	
	No or insufficient information concerning data that has not been obtained from the data subject	T4.4	When data is obtained from a third party, the data subject is not sufficiently informed about all of the following: - 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.	y	
		T4.5	The relevant information is not provided in an adequate form (e.g. easily readable and accessible).	y	
		T4.6	The relevant information is not easily understandable so that it is possible that the data subject will not be able to understand that the operator obtained information on him or her from a third party.	y	
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.	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
		T5.2	Access is possible but not to all relevant data, including: - 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.	y	
		T5.3	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before allowing access.	y	
		T5.4	Successful access as well as subsequent data disclosure is not logged.	y	
	Inability to rectify, erase or block individual data	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.	y	
		T5.6	Errors are not automatically rectified.	y	
		T5.7	There is no procedure that allows the erasure of individual data in back-up data.	y	
		T5.8	The identity of the data subject is not or not sufficiently checked (insufficient authentication) before rectification, erasure or blocking of data.	y	
		T5.9	Successful rectification, erasure and blocking is not logged.	y	
	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.	y	
T6	Inability to allow	T6.1	The data subject is not informed about	y	

Threat code and name		Sub-threat code	Description of threat	Likely (y/n)	Comments
	objection to the processing of personal data		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.		
		T6.2	A procedure (technical means and / or processes) that allows objection to the processing of personal data has not been implemented.	y	
		T6.3	The operator has not implemented any procedure that would allow the notification of relevant third parties in the case that a data subject has objected to the processing of his personal data.	y	
	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.	n	This threat belongs to P6.2, which was excluded from further consideration in step 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.	y	BSI's TG 03126 needs to be considered.
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.	y	
		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.	y	
		T8.3	The operator does not publish or does not ensure the availability of the legally defined notification contents to any person on request.	y	
		T8.4	The operator does not ensure the availability of the PIA report six weeks before the launch or upgrade of the RFID application.	y	

Table 85: Automotive-Manufacturing PIA – Identification of relevant threats

4.2.3.4 Step 5: Identification and recommendation of controls

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.1	C1.1 C1.4	SERVICE DESCRIPTION INFORMATION TIMELINESS	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.2	C1.2	INFORMATION ACCESSIBILITY	2 (P1.1)	The information describing the service is made accessible at the operator's physical facilities and online.
T1.3	C1.1	SERVICE DESCRIPTION	2 (max of P1.1 and P1.2)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.
T1.4	C1.1 C1.3	SERVICE DESCRIPTION LANGUAGE / SEMANTICS OF INFORMATION	2 (P1.1)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. 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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
T1.5	C1.4	INFORMATION TIMELINESS	2 (P1.1)	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
T1.6	C1.1 C1.2	SERVICE DESCRIPTION INFORMATION ACCESSIBILITY	2 (max of P1.1 and P1.2)	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible. The information describing the service is made accessible at the operator's physical facilities and online.
T1.7	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.8	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.9	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.10	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.11	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.12	C1.5	PRIVACY STATEMENT	2 (P1.1)	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.
T1.13	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.14	C1.6	RFID EMBLEM	2 (P1.1)	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. Additionally, it is linked with informational material describing the service and the RFID technology.
T1.15	C1.7	PURPOSE SPECIFICATION	2 (P1.2)	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.
T1.16	C1.7	PURPOSE SPECIFICATION	2 (max of P1.1 and P1.2)	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.
T1.17	C1.8	ENSURING LIMITED DATA PROCESSING	2 (P1.2)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.
T1.18	C1.8	ENSURING LIMITED DATA PROCESSING	2 (P1.3)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
	C1.9	ENSURING PURPOSE RELATED PROCESSING		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.
T1.19	C1.9	ENSURING PURPOSE RELATED PROCESSING	2 (P1.3)	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.
T1.20	C1.10	ENSURING DATA MINIMISATION	2 (P1.3)	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.
T1.21	C1.10	ENSURING DATA MINIMISATION	2 (P1.3)	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.
T1.22	C1.8	ENSURING LIMITED DATA PROCESSING	2 (P1.3)	Collected data is secured with access rights that correspond to the specified purpose. Access rights can be specified on a rather coarse-grained level.
T1.23	C1.11	ENSURING TAG PROTECTION	2 (P1.3)	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject.
T1.24	C1.12	ENSURING PERSONAL DATA QUALITY	3 (P1.4)	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.
T1.25	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3 (P1.4)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
T1.26	C1.14	ENSURING DATA ACCURACY	3 (P1.4)	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.
T1.28	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
T1.29	C1.15	ENABLING DATA DELETION	2 (P1.5)	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.
T2.1	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.2	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T2.3	C2.1	OBTAINING DATA SUBJECT'S CONSENT	3 (P2.1)	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. 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.
T4.1	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- 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.
T4.2	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.3	C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2 (P4.1)	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 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.
T4.4	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	2 (P4.2)	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, - the recipients of the data (is the data given to any third

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				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.
T4.5	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	2 (P4.2)	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, - 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.
T4.6	C4.2	PROVIDING INFORMATION ON THIRD PARTY INFORMATION PROCESSING	2 (P4.2)	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, - 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.
T5.1	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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,

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
				- 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. 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.
T5.2	C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1 (P5.1)	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: - 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. 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.
T5.3	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	1 (P5.1)	The data subject needs to identify or authenticate him or herself with his or her name and some security questions.
T5.4	C5.2	LOGGING ACCESS TO PERSONAL DATA	1 (P5.1)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T5.5	C5.3	HANDLING DATA	3	There is an application available to every data subject that

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
		SUBJECTS' CHANGE REQUESTS	(P5.2)	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.
T5.6	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	3 (P5.2)	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.
T5.7	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	3 (P5.2)	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.
T5.8	C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3 (P5.2)	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
T5.9	C5.2	LOGGING ACCESS TO PERSONAL DATA	3 (P5.2)	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
T5.10	C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	3 (P5.3)	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.
T6.1	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2 (P6.1)	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.
T6.2	C6.1	NOTIFYING DATA	2	Notifications are sent to the data subject whenever the operator

Sub-threat code	Control code(s) and name(s)		Assigned overall category (from step 3)	Description
		SUBJECTS OF SHARING PRACTICES	(P6.1)	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.
T6.3	C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2 (P6.1)	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.
T7.1	C7.1	SECURITY CONTROLS	--- (P7.1)	See relevant controls from TG 03126.
T8.1	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.
T8.2	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.
T8.3	C8.2	PRIOR CHECKING	2 (P8.1)	It is ensured that the legally required checking of the RFID application is executed by expert personnel.
T8.4	C8.1	NOTIFICATION OF AUTHORITY	2 (P8.1)	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 weeks prior to the RFID application's launch.

Table 86: Automotive-Manufacturing PIA – Identification and recommendation of controls

4.2.3.4.1 Consolidated view of identified controls

Control code and name		Highest overall category	Description
C1.1	SERVICE DESCRIPTION	2	Extensive informational material (e.g. flyers, RFID emblem, websites) is made available that is easily understandable and accessible.
C1.2	INFORMATION ACCESSIBILITY	2	The information describing the service is made accessible at the operator's physical facilities and online.
C1.3	LANGUAGE / SEMANTICS OF INFORMATION	2	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). The information describing the service is available in the most common languages and in languages that are potentially specific to its target countries.
C1.4	INFORMATION TIMELINESS	2	The information describing the service is checked at regular intervals for its timeliness, especially when questions from data subjects could not be answered.
C1.5	PRIVACY STATEMENT	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.
C1.6	RFID EMBLEM	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.
C1.7	PURPOSE SPECIFICATION	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.
C1.8	ENSURING LIMITED DATA PROCESSING	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.
C1.9	ENSURING PURPOSE RELATED PROCESSING	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.
C1.10	ENSURING DATA MINIMISATION	2	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.

Control code and name		Highest overall category	Description
C1.11	ENSURING TAG PROTECTION	2	RFID tags are deactivated, killed or cryptographically secured before they are handed to the data subject.
C1.12	ENSURING PERSONAL DATA QUALITY	3	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.
C1.13	ENSURING DATA SUBJECT AUTHENTICATION	3	The data subject needs to identify or authenticate himself with a valid ID or eID, either personally or online.
C1.14	ENSURING DATA ACCURACY	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	ENABLING DATA DELETION	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.
C2.1	OBTAINING DATA SUBJECT'S CONSENT	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.
C4.1	PROVIDING INFORMATION PROCESSING INFORMATION	2	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 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.
C4.2	PROVIDING INFORMATION ON THIRD PARTY	2	When data is obtained from a third party, the data subject has access to information that describes all relevant data:

Control code and name		Highest overall category	Description
	INFORMATION PROCESSING		- 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.
C5.1	INFORMING DATA SUBJECTS ABOUT DATA PROCESSING	1	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: - 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. 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.
C5.2	LOGGING ACCESS TO PERSONAL DATA	3	Data subjects' access to data, subsequent data disclosure, rectification, erasure and blocking are logged on a level that is sufficient to ensure accountability.
C5.3	HANDLING DATA SUBJECTS' CHANGE REQUESTS	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.

Control code and name		Highest overall category	Description
C6.1	NOTIFYING DATA SUBJECTS OF SHARING PRACTICES	2	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.
C7.1	SECURITY CONTROLS	---	See relevant controls from TG 03126.
C8.1	NOTIFICATION OF AUTHORITY	2	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 weeks prior to the RFID application's launch.
C8.2	PRIOR CHECKING	2	It is ensured that the legally required checking of the RFID application is executed by expert personnel.

Table 87: Automotive-Manufacturing PIA – Consolidated view of identified controls

4.2.3.5 Step 6: Documentation of residual risks

For technical or business reasons it is not always possible to eliminate threats completely by applying controls. Some residual risks remain. These residual risks should be documented in this step. It is recommended to provide a comprehensive description and an evaluation (low, medium, high) for each residual risk.

5 Bibliography

[ART2007] Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. WP 136. 20 June 2007.

[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.