Privacy and Data Protection Impact Assessment Framework for RFID Applications

12 January 2011

INDEX

1. Introduction

The European Commission ("the Commission") issued a Recommendation dated 12 May 2009 on the implementation of privacy and data protection principles in Applications supported by Radio Frequency Identification ("RFID Recommendation"). In that Recommendation, the Commission established a requirement for the endorsement by the Article 29 Data Protection Working Party of an industry-prepared framework for Personal Data and Privacy impact assessments of RFID Applications. These assessments are commonly referred to as privacy impact assessments, or PIAs. This RFID Application PIA Framework ("the Framework") addresses that requirement.

The benefits of conducting PIAs for RFID Applications are numerous. These include helping the RFID Application Operator:

- to establish and maintain compliance with privacy and data protection laws and regulations;
- to manage risks to its organisation and to users of the RFID Application (both privacy and data protection compliance-related and from the standpoint of public perception and consumer confidence); and
- to provide public benefits of RFID Applications while evaluating the success of privacy by design efforts at the early stages of the specification or development process.

The PIA process is based on a privacy and data protection risk management approach focusing mainly on the implementation of the EU RFID Recommendation and consistent with the EU legal framework and best practices.

The PIA process is designed 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. These impacts (if any) could vary significantly, depending on the presence or lack of personal information processing by the RFID Application. The PIA Framework provides guidance to RFID Application Operators on the risk assessment methods, including adequate measures to mitigate any likely data protection or privacy impact in an efficient, effective and proportionate manner.

Finally, the PIA Framework is sufficiently general to be applicable to all RFID Applications, while allowing for particularities and specificities to be addressed at Sectoral or Application type level.

The PIA Framework is part of the context of other information assurance, data management, and operational standards that provide good data governance tools for RFID and other Applications. The current Framework could be used as a basis for the development of industry-based, sector-based, and/or application-based PIA templates. As in the implementation of any theoretical document, the PIA Framework may require clarification of its application of terms, as well as guidance on practices that should be based on practical experience, that may help in its implementation.

1.1. Key Concepts

There are a number of key concepts used in the Framework that warrant description. ***RFID*** is a technology that uses electromagnetic waves to communicate with RFID Tags, with the possibility of reading the unique identification numbers of the RFID Tags or perhaps other information stored in them. ***RFID Tags*** are generally small and can take many forms, but are often composed of electronic memory that is readable and perhaps writable, and antennae. ***RFID Readers*** are used to read the information on RFID Tags.

RFID Applications process information developed through the interaction of RFID Tags and RFID Readers. Such Applications are operated by one or more ***RFID Application Operators*** and are supported by back-end systems and networked communication infrastructures. If an RFID Application Operator makes determinations related to the collection or use of personal data, its role could be similar to that of the Data Controller as defined in Directive 95/46/EC and would be described as the 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 RFID Application which has impacts or personal information.

In the context of RFID technology, the following taxonomy applies:

- A ***Privacy Impact Assessment (PIA)*** is a process whereby a conscious and systematic effort is made to assess the privacy and data protection impacts of a specific RFID Application with the view of taking appropriate actions to prevent or at least minimise those impacts.
- The ***Framework*** identifies the objectives of RFID Application PIAs, the components of RFID Applications to be considered during PIAs, and the common structure and content of RFID Application PIA Reports.
- A ***PIA Report*** is the document resulting from the PIA Process that is made available to competent authorities. Proprietary and security sensitive information may be removed from PIA Reports before the Reports are provided externally (e.g., to the competent authorities) as long as the information is not specifically pertinent to privacy and data protection implications. The manner in which the PIA should be made available (e.g., upon request or not) will be determined by member states. In particular, the use of special categories of data may be taken into account, as well as other factors such as the presence of a data protection officer.
- ***PIA Templates*** may be developed based on the Framework to provide industry-based, application-based, or other specific formats for PIAs and resulting PIA Reports.

These and other terms, such as ***Users*** **and** ***Individual***, are for the purpose of this PIA Framework also described in Appendix B: Glossary. Terms from Directive 95/46/EC related to data protection are incorporated by reference.

The execution and reporting, where appropriate, of PIAs are in addition to other obligations that the RFID Application Operators may have under specific applicable laws, regulations, and other binding agreements.

1.2. Internal Procedures

RFID Application Operators should have their own internal procedures to support the execution of PIAs, such as the following:

- *Scheduling of the PIA process* so that there is sufficient time to make any needed adjustments to the RFID Application and to make the PIA Report available to the competent authorities at least six weeks before deployment.
- *Internal review of the PIA process (including the initial analysis) and PIA Reports* for consistency with other documentation related to the RFID Application, such as system documentation, product documentation, and examples of product packaging and RFID Tag implementation. The internal review should provide a feedback loop to address any impacts collected after the Application is implemented and to accommodate results from prior PIAs.

- *Compilation of supporting artefacts* (that may include results of security reviews, controls designs and copies of notices) as evidence that the RFID Application Operator has fulfilled all of the applicable obligations.
- *Determination of the persons and/or functions within the organisation who have the authority for relevant actions* during the PIA process (e.g., completion of the PIA initial analysis and PIA Report, signing the PIA Report, maintaining applicable documents, and any separation of duties for these functions).
- *Provision of criteria for how to evaluate and document whether the Application is ready or not ready for deployment* consistent with the Framework and any relevant PIA Template.
- *Consideration/Identification of factors that would require a new or revised PIA Report* is warranted. Criteria should 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[1] 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. Material changes that would narrow the scope of collection or use would not trigger per se the need for a revised PIA. Throughout the lifetime of the RFID Application, a new or revised PIA Report would be warranted if the RFID Application changes in level as described in the Initial Analysis Section.
- *Stakeholder Consultation.* Opinions and feedback from relevant stakeholders related to the RFID Application under review should be appropriately considered as part of the PIA review of potential concerns and issues. Consultations should be appropriate to the scale, scope, nature, and level of the RFID Application. Within companies, individuals are designated with responsibility for overseeing and assuring organisational or departmental privacy. These individuals are essential participants in the PIA process to the extent that they are involved in the particular RFID Applications or their oversight. Employees with knowledge of technical, marketing and other disciplines may also be needed participants in the process, depending upon the nature of the RFID Application and their relation to it. RFID Operators may have consultation mechanisms by which external stakeholders, whether individuals, organisations or authorities, can interact with them and provide feedback. As far as is appropriate, the RFID Operator should use consultation mechanisms to gain input from the groups representing the individuals whose privacy will be directly impacted by the proposals, e.g. employees and customers of the RFID operator.

2. The PIA Process

The purpose of the Framework is to provide guidance to RFID Application Operators for conducting PIAs on specific RFID Applications, as called for in the Recommendation, and to define the common organisational structure and content categories of the PIA Reports in which the results from such PIAs have to be documented. In addition, because many RFID Application Operators within particular sectors may be considering the same or similar RFID Applications, the Framework provides a basis for the development of PIA Templates for particular Applications or industry sectors. PIA Templates can assist these sectors to conduct PIAs and produce the resulting PIA Reports for these similar RFID Applications

[1] In this case the applicable definition shall be the one provided in the directive 2009/136/EC amending directive 2002/58 see page 29 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

more efficiently[2]. Because common RFID Applications may be offered in a number of Member States, the Framework is designed to harmonise requirements for RFID Application Operators consistent with local laws, regulations, best practices and other binding agreements.

The Framework addresses the process for conducting PIAs of RFID Applications before deployment and specifies the scope of resulting PIA Reports.[3]

RFID Application Operators must develop a PIA for each RFID Application they operate. If they deploy several related RFID Applications (potentially in the same context or at the same premises) they may create one PIA Report if the boundaries and differences of the Applications are explicitly described in the PIA Report. If RFID Application Operators reuse one RFID Application in the same way for multiple products, services or processes, they may create one PIA Report for all products, services or processes that are similar (for example, a car manufacturer deploying the same anti-theft mechanisms in all cars and under the same service conditions). The execution and reporting, where appropriate, of PIAs are in addition to other obligations that the RFID Application Operators may have under specific applicable laws, regulations, and other binding agreements.

The PIA process has two phases:

1. **Initial Analysis Phase**: the RFID Application Operator will follow the steps outlined in this Section to determine:

    a) whether a PIA of its RFID Application is required or not; and

    b) if a Full or Small Scale PIA is warranted.

2. **Risk Assessment Phase**: it outlines the criteria and elements of Full and Small Scale PIAs.

2.1. Initial Analysis Phase

As a prerequisite to conducting a PIA for a specific Application, each organisation must understand how to implement such a process based on the nature and sensitivity of the data it deals with, the nature and type of processing or stewardship of information it engages in, and the type of RFID Application in question. For those organisations that may already have privacy risk assessment processes in place for other Applications, the classification criteria and process steps should help them map their existing PIA processes to this Framework.

To conduct the initial assessment, an RFID Application Operator has to go through the decision tree depicted in Figure 1. This will help the RFID Application Operator to determine whether and to what extent a PIA is needed for the RFID Application at hand.

The resulting level in the initial analysis phase helps determine the level of detail necessary in the risk assessment (e.g., either a Full Scale or Small Scale PIA).

This initial analysis must be documented and made available to data protection authorities upon request. For documentation guidelines, please see Annex I.

---

[2] The concept of mutual or multiple recognition across entities and sectors for the deployment of previously vetted RFID Applications should be explored.

[3] Point 5 (a) of the European Commission Recommendation of May 2009 on the implementation of privacy and data protection principles in Applications supported by radiofrequency identification C(2009) 3200 final.

Full Scale PIA

A Full Scale PIA is required for Applications that are determined to be Level 2 or Level 3 by the initial analysis phase in Section 2.1. Examples of Applications requiring a Full Scale PIA include Applications that process personal information (Level 2) or where the RFID Tag contains personal data (Level 3). While both Level 2 and Level 3 result in a Full Scale PIA, they identify different risk environments and as such will have different mitigation strategies. For example, Level 2 Applications may have controls to protect back-end data while Level 3 Applications may have controls to protect both back-end data and tag data. Industry may further refine these levels and how they impact the PIA process with further experience. Since the Application processes personal data, a highly detailed risk assessment (Full Scale) is necessary to ensure that mitigations are well elaborated. This will help the RFID Application Operator to identify relevant risks and develop appropriate controls. In this context, Operators should also consider whether the RFID Tag's information is likely to be used beyond the initial purpose or context understood by the individual, particularly if it could be used to process or link to personal data, and whether a new PIA analysis is warranted or other mitigating controls should be employed.

Small Scale PIA

Small Scale PIAs follow the same process as Full Scale PIAs, but given the lower risk profile a Small Scale PIA is more restricted in scope and level of detail in both the inquiry and the report than a Full Scale PIA. Small Scale PIAs are relevant for Level 1 Applications. While a Small Scale PIA follows a similar process to the Full Scale PIA, since the relevant risks of a Level 1 Application are lower than Level 2 or Level 3, the required controls and corresponding documentation in the PIA Report are simplified.

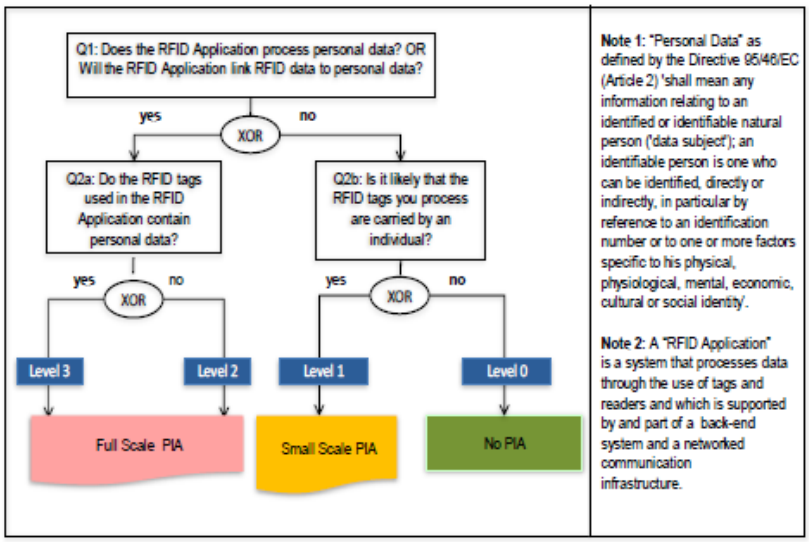


Figure 1: Decision Tree on whether and at what level of detail to conduct a PIA

2.2. Risk Assessment Phase

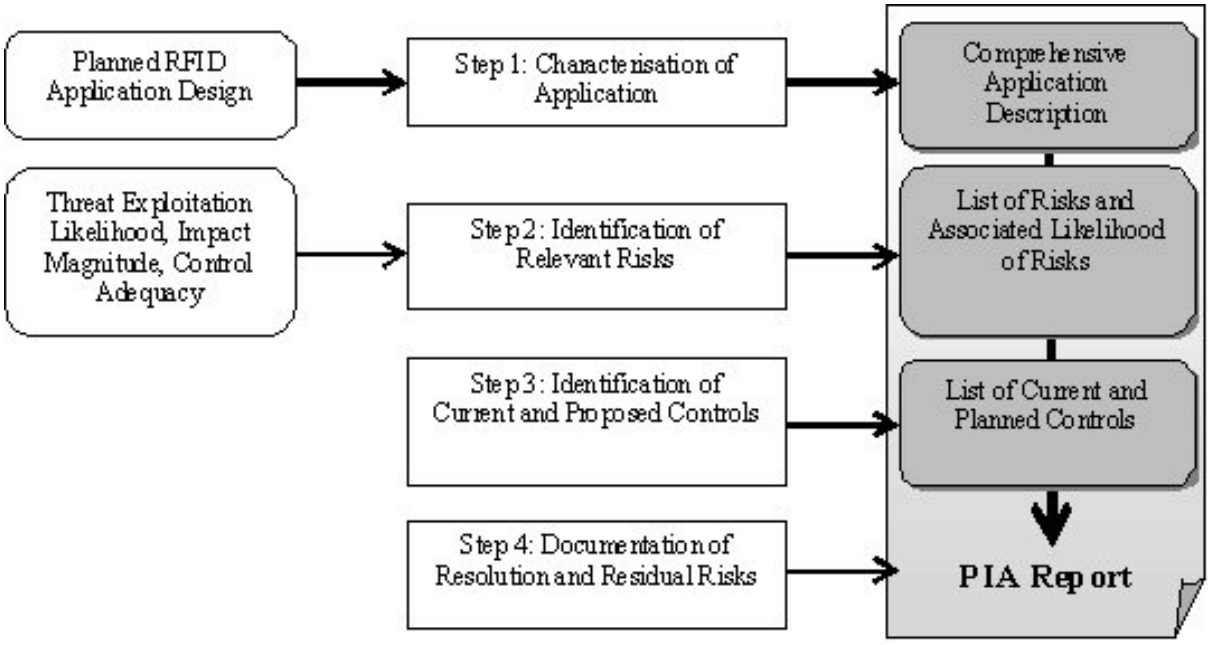
The objective of a risk assessment is to identify the privacy risks caused by an RFID Application - ideally at an early stage of system development - and to document how these risks are *pro-actively* mitigated through technical and organisational controls. In this way a PIA plays an important role in compliance and the legal requirements of privacy (Directive 95/46) and is a measure by which we judge the effectiveness of the mitigation procedures.

To save time and cost, it is recommended to run through this risk assessment phase well before final decisions on an RFID Application's architecture are taken so that technical privacy mitigation strategies can be embedded into the system's design, and do not need to be 'bolted on' later.

A risk assessment process typically considers in the first instance the risks of an RFID Application in terms of their likelihood of occurrence and magnitude of their consequences. RFID Application Operators are advised to use the privacy targets of the EU Directive as a starting point for their risk assessment (see Annex II). Privacy risks may be high, because the RFID Application implementation could be susceptible to malicious attacks or because organisational or environmental privacy controls do not exist. Privacy risks may also be small, simply because their occurrence is unlikely in the environment or organisation at hand, or because the RFID Application is already configured in a highly privacy friendly way. The PIA Process aims to consider all potential risks and then reflects on their magnitude, likelihood and potential mitigation. The result of this reflection is the identification of those privacy risks that are really relevant for the organisation's RFID deployment and that need to be mitigated through effective controls.

The PIA Process (as visualised in figure 2) requires any RFID Application Operator to:

1. Describe the RFID Application;
2. Identify and list how the RFID Application under review could threaten privacy and estimate the magnitude and likelihood of those risks;
3. Document current and proposed technical and organisational controls to mitigate identified risks; and
4. Document the resolution (results of the analysis) regarding the Application.



Step 1: Characterisation of Application

The Application characterisation should give a comprehensive and full picture of the Application, its environment and system boundaries. The Application design, its adjacent interfaces with other systems, and information flows are described. Data flow diagrams that show processing of primary and secondary data are recommended to visualise information flows. Data structures need to be documented, too, so that potential links can be analysed. Annex I summarises the elements that characterise an RFID Application for the purposes of conducting a PIA.

In addition, information related to the Application's operational and strategic environment is recommended. This may include the system's immediate and longer-term mission, stakeholders in information collection, functional requirements, all potential users and a description of the RFID Application's architecture and data flows (in particular, interfaces to external systems that may process personal data).

Step 2: Identification of Risks

The goal of this step is to identify conditions that may threaten or compromise personal data using the EU Directive as a guide for important hallmarks of privacy targets to protect. Risks may be related to the RFID Application components, its operations (collection, storage and processing infrastructure) and the data sharing and processing environment in which it is embedded.

A list of potential privacy risks may be found in Annex III. They serve as a guide for a systematic identification of potential risks that threaten the EU Directive targets (Annex II).

In addition to the identification of risks, a PIA requires a relative quantification of these risks. An RFID Application Operator should consider, as informed by the principles of proportionality and under reasonable terms, the *likelihood* of privacy risks occurring. Risks can occur from within, and where warranted, outside of the particular RFID Application at hand. These risks may be derived from both the likely uses and possible misuses of the information, and in particular if the RFID Tags used within the RFID Application remain operational once in possession of individuals**.**

The risk assessment requires evaluating the applicable risks from a privacy perspective; the RFID Operator should consider:

1. The significance of a risk and the likelihood of its occurrence.
2. The magnitude of the impact should the risk occur.

The resulting risk level can then be classified as low, medium or high.

A risk that has caused a prime subject of debate is that RFID Tags could be used for the profiling and/or tracking of individuals. In this case the RFID Tag's information – in particular its identifier(s) – would be used to re-identify a particular individual. Retailers who pass RFID Tags on to customers without automatically deactivating or removing them at the checkout *may* unintentionally enable this risk. A key question, though, is whether this risk is likely and actually materialises into an *undismissable* risk or not. According to point 11 of the RFID Recommendation, retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy in accordance with this Framework, give their consent to keep the tags operational. Retailers are not required to deactivate or remove tags if the PIA report concludes that tags that are used in a retail application and would remain operational after the point of sale do not represent a likely threat to privacy or the protection of personal data as stated in point 12 of the same

Recommendation. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer.

Sector specific templates that shall be developed over time on the basis of this Framework and for use in different industries may inform risk identification in greater detail.

Step 3: Identification and Recommendation of Controls

The goal of this step is to analyse the controls that have been implemented or are planned for implementation, to minimise, mitigate or eliminate the identified privacy risks.

Controls are either of a technical or nontechnical nature. Technical controls are incorporated into the Application through architectural choices or technically enforceable policies, e.g. default settings, authentication mechanisms, and encryption methods. Nontechnical controls on the other hand are management and operational controls, e.g. operational procedures. Controls can be categorised as being preventive or detective. The former ones inhibit violation attempts and the latter ones warn of violations or attempted violations.

There can also be 'natural' controls created by the environment. For example, if there are no readers installed that could conduct a tracking of items or individuals (i.e. because there is no business case for it), then naturally there is also no (likely) risk.

The identified risks and their associated risk levels should guide the decision on which of the identified controls are relevant and thus need to be implemented. The PIA documentation should explain how the controls relate to specific risks, and should elaborate on how this mitigation will result in an acceptable level of risk.

Examples of controls are provided in Annex IV.

Step 4: Documentation of Resolution and Residual Risks

Once the risk assessment has been completed, the final resolution about the Application should be documented in the PIA Report, along with any further remarks concerning risks, controls and residual risks.

- An RFID Application is approved for operations once the PIA Process has been completed with relevant risks identified and appropriately mitigated to assure no significant residual risks remain in order to meet the requirements of compliance, with appropriate internal reviews and approvals.

- Where an RFID Application is not approved for operations in its current state, further consideration will require a specific corrective action plan to be developed, and a new privacy impact assessment to be completed in order to determine if the Application has reached an approvable state.

The resolution should be associated with the following information:

- Name of the person signing the resolution.
- Title of the person.
- Date of the resolution.

PIA Report

PIAs are internal processes containing sensitive information that can have security implications as well as potentially confidential and proprietary information of the company related to products and processes. That said, a PIA report should typically include:

1. The Description of the RFID Application as outlined in ANNEX I.

2. Documentation of the four steps outlined above.

The signed PIA Report that contains an approved resolution should be given to the assigned company's data privacy/security official in accordance with the RFID Application Operator's internal procedures. This report is provided without prejudice to the obligations set forth in the Directive 95/46/EC for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC.

3. Final Provision

The PIA Framework will take effect no later than 6 months after publication and endorsement by the Article 29 Data Protection Working Party. For RFID Applications in place before the PIA Framework takes effect, the PIA Framework will apply only when the conditions are met for documenting a new or revised PIA in accordance with the PIA Framework.

ANNEX I - *Characterisation of the RFID Application Description*

The RFID Application Operator should include, where applicable, the below information in the PIA Report.

RFID Application Operator	• Legal entity name and location • Person or office responsible for PIA timeliness • Point(s) of contact and inquiry method to reach the Operator
RFID Application Overview	• RFID Application name • Purpose(s) of RFID Application(s) • Basic use case scenarios of the RFID Application • RFID Application components and technology used (i.e. Frequencies, etc.) • Geographical scope of the RFID Application • Types of users/individuals impacted by the RFID Application • Individual access and control
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 • Presence of Sensitive information in the data being processed, e.g., health
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 the personal data
External RFID Data Transfer (if applicable)	• Type of data recipient(s) • 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)

ANNEX II - *Privacy Targets*

There are today 9 privacy targets embedded in the Directive 95/46/EC. The PIA Process was developed by considering these targets and the associated risks of RFID. This Annex summarises these privacy targets. While all targets are essential elements of organisational compliance, in many cases only a subset of these requirements will be at issue in the RFID Application under consideration. Thus the role of these targets is to inform the creation and development of the PIA process more than the operation of any specific PIA.

Description of privacy target (taken and updated from the respective EU Privacy Directive(s); here Directive 95/46/EC)	
Safeguarding quality of personal data	Data avoidance and minimisation, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on consent, contract, legal obligation, etc.
Legitimacy of processing *sensitive* personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner.
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially.
Safeguarding confidentiality and security of processing	Preventing unauthorised access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured.
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured.
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.

ANNEX III - *Privacy Risks*

This section provides a list of possible privacy risks related to the use of the RFID Application under review. It is recommended that – in particular for Full Scale PIAs - risks are systematically identified with the help of standard risk assessment procedures that would include threats and vulnerabilities to an RFID Application.

The table below provides examples of risks that may affect an entity's ability to meet the privacy targets described in Annex II. RFID Application Operators can use this list as a starting point; however, not all of these risks may apply to all RFID Applications. RFID Operators should make sure each identified risk is appropriately mitigated by one or more controls in light of the likelihood of risk occurrence and magnitude of impact. RFID Application Operators may need to combine controls or augment existing controls based on factors including the technology in use, nature of their implementation, type of information, and applicable policies, among others.

Privacy Risk	Description and example
Unspecified and unlimited purpose	The purpose of data collection has not been specified and documented or more data is used than is required for the specified purpose. Example: No documentation of purposes for which RFID data is used and/or use of RFID data for all kinds of feasible analysis.
Collection exceeding purpose	Data is collected in identifiable form that goes beyond the extent that has been specified in the purpose. Example: RFID payment card information is not only used for the purpose of processing transactions but also to build individual profiles.
Incomplete information or lack of transparency	The information provided to the data subject on the purpose and use of data is not complete, data processing is not made transparent, or information is not provided in a timely manner. Example: RFID Information available to consumers that lacks clear information on how RFID data is processed and used, the identity of the Operator, or the user's rights.
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose. Example: RFID payment card information is combined with personal data obtained from a third party.
Missing erasure policies or mechanisms	Data is retained longer than necessary to fulfil the specified purpose. Example: Personal data is collected as part of the Application and is saved for longer than

	legally allowed.
Invalidation of explicit consent	Consent has been obtained under threat of disadvantage. Example: Cannot return/exchange/use legal warranties for products when RFID Tag is deactivated or removed.
Secret data collection by RFID Operator	Some data is secretly recorded and thus unknown to the data subject, e.g. movement profiles. Example: Consumer information is read while walking in front of stores or in mall and no Logo or Emblem is warning him or her about RFID readouts.
Inability to grant access	There is no way for the data subject to initiate a correction or erasure of his data. Example: Employer cannot give employee a full picture of what is saved about him or her on the basis of RFID access and manufacturing data.
Prevention of objections	There are no technical or operational means to allow complying with a data subject's objection. Example: Hospital visitor cannot opt out of reading out sensitive personal information on tags (i.e. medications).
A lack of transparency of automated individual decisions	Automated individual decisions based on personal aspects are used but the data subjects are not informed about the logic of the decision-making. Example: Without notice to consumers, an RFID Operator reads all tags carried by an individual, including tags provided by another entity, and determines what type of marketing message the individual should receive based on the tags.
Insufficient access right management	Access rights are not revoked when they are no longer necessary. Example: Through an RFID card, an ex-trainee gets access to parts of an enterprise where he or she should not.
Insufficient authentication mechanism	A suspicious number of attempts to identify and authenticate are not prevented. Example: Personal data contained on tags is not protected by default with a password or another authentication mechanism.
Illegitimate data processing	Processing of personal data is not based on consent, a contract, legal obligation, etc. Example: An RFID Operator shares collected information with a third party without notice or

	consent as otherwise legally allowed.
Insufficient logging mechanism	The implemented logging mechanism is insufficient. It does not log administrative processes. Example: It is not logged who has accessed the RFID employee card data.
Uncontrollable data gathering from RFID Tags	The risk that RFID Tags could be used for regular profiling and/or tracking of individuals. Example: Retailer reads all tags that they can see.

ANNEX IV – *List of Examples of RFID Application Controls and Mitigating Measures*

This section provides a list of examples of potential controls that can help an RFID Application Operator to identify appropriate mitigating strategies. Risks identified as relevant for an RFID Application Operator in Step 2 of the PIA risk process can be mitigated through one or several mitigation strategies, some of which are outlined in this Annex IV. The goal is that by running through a PIA process, the RFID Application Operator identifies and implements the controls necessary to mitigate the relevant privacy risks.

Potential control mechanisms include:

- RFID Application Governing Practices.
- Individual access and control.
- System Protection Measures (including Security Controls).
- Tag Protection.
- Accountability Measures.

These practices are ancillary to the existing European Union data protection regulatory framework and are not intended to replace it or modify its scope.

RFID Application Governing Practices

Governing practices may include:

- Management practices by the RFID Application Operator.
- Disposal of and erasure policies for RFID data.
- Policies related to lawful processing of personal information.
- Provisions in place for data minimisation in handling RFID data, where feasible.
- Processing or storing of information from tags that do not belong to the RFID Operator.
- Security Governance practices.

Providing Individual Access and Control

- Providing information about the purposes of the processing and the categories of personal data involved.
- Description of how to object to the processing of personal data or withdraw consent.
- Identification of process to request rectification or erasure of incomplete or inaccurate personal data.

System Protection

System Protection with respect to the appropriate protection of privacy and personal data should also be documented in this Section of the PIA Report. System protection concepts apply to back-end systems and communication infrastructure in so far as they are relevant to the RFID Application. Where they do apply, it should be recognised that backend systems are often complex and may have been the subject of their own PIA. That analysis may need to be reviewed to assure that it considered information of the nature used by the RFID Application. Where no such PIA exists, the following components of the backend system should be considered:

- Access controls related to the type of personal data and functionality of the systems are in place.
- Controls and policies put in place to ensure the Operator does not link personal data in the RFID Application in a manner inconsistent with the PIA Report.
- Whether appropriate measures are in place to protect the confidentiality, integrity, and availability of the personal data in the systems and in the communication infrastructure.
- Policies on the retention and disposal of the personal data.
- Existence and implementation of information security controls, such as:
    - Measures that address the security of networks and transport of RFID data.
    - Measures that facilitate the availability of RFID data through appropriate back-ups and recovery.

RFID Tag Protection

RFID Tag Protection controls related to privacy and personal data should be indicated. They are particularly relevant to RFID Applications that use RFID Tags containing personal data.

These protection controls include the following:

- Access control to functionality and information, including authentication of readers, writers, and underlying processes, and authorisation to act upon the RFID Tag.
- Methods to assure/address the confidentiality of the information (e.g., through encryption of the full RFID Tag or of selective fields).
- Methods to assure/address the integrity of the information.
- Retention of the information after the initial collection (e.g., duration of retention, procedures for eliminating the data at the end of the retention period or for erasing the information in the RFID Tag, procedures for selective field retention or deletion).
- Tamper resistance of the RFID Tag itself.
- Deactivation or removal, if required or otherwise provided.

Mitigation can include user based controls that address situations where different needs or sensitivities related to privacy may be at issue. Deactivation or removal are currently the two most common forms of end-user/consumer mitigation. These may either be required as part of a PIA analysis, in certain circumstances by law or as a customer option after the point of sale to enhance confidence. In addition, the EC Recommendation on RFID Privacy and Data Protection for RFID Applications suggests certain methodologies and best practices associated with implementation of deactivation or removal in retail.[4]

Accountability Measures

These measures are designed to address procedural data protection, in the area of accountability. Through these measures external awareness regarding RFID Applications is raised.

- Ensuring the easy availability of a comprehensive **information policy** that includes:
    - Identity and address of the RFID Application Operator.
    - Purpose of the RFID Application
    - Types of data processed by the RFID Application, in particular if personal data are processed.
    - Whether the locations of RFID Tags will be monitored when possessed by an individual.
    - Likely privacy and data protection impacts, if any, relating to the use of RFID Tags in the RFID Application and the measures available to mitigate these impacts.
- Ensuring concise, accurate and easy to understand **notices** of the presence of RFID readers that include:
    - The identity of the RFID Application Operator.
    - A point of contact for Individuals to obtain the information policy.
- Noting if and how **redress mechanisms** are made available:
    - RFID Application Operator accountable legal entity (-ies) (may be one for each jurisdiction or operating area).
    - Point(s) of contact of the designated person or office responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures related to the protection of personal data and privacy.
    - Inquiry methods (e.g., methods through which the RFID Application Operator may be reached to ask a question, make a request, file a complaint, or exercise a right).

[4] Point 12/13 of the EC Recommendation of 12 May 2009. {SEC (2009) 585}: *Any deactivation or removal method should be made available free of charge, either immediately or at a later stage, without any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer.*

- Methods to object to processing, to exercise access rights to personal data (including deleting and correcting personal data), to revoke consent, or to change controls and other choices regarding the processing of personal data, if required or otherwise provided.

- Other redress methods, if required or otherwise provided.

Appendix A: References

This Section provides references to formal documents used to help develop the Framework.

- "Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio-frequency identification," Commission of the European Communities, 12 May 2009, C (2009) 3200, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

- "Commission staff working document accompanying the Commission Recommendation on the implementation of privacy and data protection principles in Applications supported by radio frequency identification," Summary of the Impact Assessment, Commission of the European Communities, 12 May 2009, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

- "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of Individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Communities, 23 November 1995, L 281/31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

- "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Official Journal of the European Communities, 31 July 2002, L 201/37, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

- "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws," Official Journal of the European Union, 18 December 2009, *L* 337/11, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF

- "Opinion 4/2007 on the concept of personal data," Article 29 Data Protection Working Party, 20 June 2007, 01248/07/EN WP 136, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

- "Privacy Impact Assessment Handbook," available at http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

- "Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data," available at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

- "Working document on data protection issues related to RFID technology," Article 29 Data Protection Working Party, 19 January 2005, 10107/05/EN WP 105, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

Appendix B: Glossary

A number of terms are used in the Framework related to the concepts of privacy and data protection, and to the Application of RFID technology in a wide range of contexts. For the purposes of this Framework, the definitions set out in Directive 95/46/EC should apply regarding privacy and data protection.

The following definitions relate to RFID technology and its Application, and are relevant to the Framework:

Individual. A natural person who interacts with or is otherwise involved with one or more components of an RFID Application (e.g., back-end system, communications infrastructure, RFID Tag), but who does not operate an RFID Application or exercise one of its functions. In this respect, an Individual is different from a User. An Individual may not be directly involved with the functionality of the RFID Application, but rather, for example, may merely possess an item that has an RFID Tag.

Information Security. Preservation of the confidentiality, integrity and availability of information.

Monitor. Carrying out an activity for the purpose of detecting, observing, copying or recording the location, movement, activities, or state of an Individual.

Personal Data. 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.

RFID Application. 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.

RFID Application Operator. The 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.

Radio Frequency Identification (RFID). The use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

RFID Reader. A fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.

RFID Tag or 'tag'. An RFID device having the ability to produce a radio signal or an RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer.

RFID Tag Information or information on the RFID Tag. The information contained in an RFID Tag and transmitted when the RFID Tag is queried by an RFID Reader.

User. Specifically, an RFID Application User, i.e., a person (or other entity, such as a legal entity) who directly interacts with one or more components of an RFID Application (e.g., back-end system, communications infrastructure, RFID Tag) for the purposes of operating an RFID Application or exercising one or more of its functions.