Appendix 1: The proposed Framework

Industry Proposal
Privacy and Data Protection Impact Assessment Framework for RFID Applications

March 31 2010

Contents

Preface 3

1. *Introduction* 4

1.1 *Purpose* 4

1.2 *Applicability* 5

1.3 *Key Concepts* 5

1.4 *Internal Procedures* 6

1.5 *Classification criteria of RFID Applications* 7

2. *The PIA Process* 9

2.1 *Initial Analysis* 9

2.2 *PIA Report Structure and Content* 9

2.3 *Part A: RFID Application Description and Scope* 10

2.3.1 RFID Application Operator 11

2.3.2 Other Parties and Users of the RFID Application 11

2.3.3 RFID Application Description 11

2.3.4 Individuals and Users Interacting with the RFID Application 12

2.3.5 Presence of Personal Data in the RFID Application 12

2.3.6 RFID Application Data Flows 13

2.3.7 RFID Application Classification 14

2.4 *Part B: RFID Application Governing Practices* 14

2.4.1 Individual Access and Control 14

2.4.2 System Protection 15

2.4.3 RFID Tag Protection 16

2.4.4 Access and Transfers to Other Parties 16

2.4.5 Adequacy of Transfers Outside the European Economic Area (EEA) 16

2.5 *Part C: Accountability* 17

2.5.1 Transparency and information 17

2.5.1.1 Published Information Policy 17

2.5.1.2 Notice 17

2.5.1.3 Other Stakeholders 17

2.5.2 Redress Methods 18

2.5.3 Regulatory Compliance 18

2.5.4 PIA Report Initiation and Updates 18

2.6 *Part D: Analysis and Resolution* 18

3. *Final Provision* 19

Appendix A: References 20

Appendix B: Glossary 22

Appendix C: The PIA Process 24

1. Preface

The Privacy Impact Assessment (PIA) Framework through its guidance, structure and elements, provides Radio Frequency Identification (RFID) Application Operators with a significant tool to guide their implementation of the PIA requirement as spelled out in the European Commission's RFID Recommendation.

A PIA is a practical privacy and data protection risk tool that helps evaluate how well principles of privacy have been implemented in the design phase of a system – "built in" rather than "bolted on."

While the privacy principles underlying PIAs are common to many regional and international instruments on privacy, the PIA itself must be tailored to examine privacy in the system as implemented, thus a PIA is focused on the objectives and functions of the type of system under review.

Our objective in developing the PIA Framework is that it both responds to the PIA provisions of the Recommendation and is deployable and manageable for those executing the PIAs as well as those reviewing them.

The PIA Framework, as the Recommendation it is based on, provides for private sector and regulatory components with respective yet interdependent roles and responsibilities. Thus to serve its purpose, the PIA process must result in outcomes that both meet the needs of regulators while being operationally efficient and encouraging RFID Operators, regardless of their size and sector, to conduct PIAs. The PIA tool should be seen as an incentive for organisations to deploy privacy-friendly Applications to reassure the relevant stakeholders either that their RFID Applications have no privacy implications or that the proper measures and controls are in place when implications for privacy and data protection do exist. Conversely, it should not impose a burden that would limit European competitiveness or innovation related to the technology.

The PIA Framework is just what its name implies - a Framework that sets the parameters for conducting PIA Reports for specific Applications, or for establishing PIA Templates to be used by an industry. The level of documentation required in the PIA Report will necessarily vary depending on the privacy implications of the specific RFID Application under review, taking into account its nature, characteristics and the mitigating measures in place. This PIA Framework recognises that a commitment to responsible use of RFID technology is not at odds with maintaining and increasing the levels of competitiveness of European industry as a whole. Mechanisms for reporting PIAs to the competent authorities need to be proportionate and operationally efficient, in particular for those types of RFID Supply Chain Systems and Applications which by their nature strictly operate in business to business environments and do not implicate privacy. The high volume of PIA Reports of supply chain systems and Applications might undermine the capacity of the competent data protection authorities to review the PIAs of RFID Applications that do implicate privacy.

Based on the above and notwithstanding the fact that the draft PIA Framework addresses all kinds of RFID Applications, further consideration is needed to balance the administrative burden of the level of detail of PIA Reports against the real privacy and data protection impacts of these Applications.

Finally, the draft PIA Framework allows for the development of sector-specific Templates to help RFID Operators with the operational aspects of conducting PIAs of their specific RFID Applications.

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 stand point of public perception and consumer confidence), and
- To provide public benefits of RFID Applications while integrating privacy by design at the early stages of the specification or development process.

The PIA process as defined in Section 2 is based on a privacy and data protection risk management approach, focussing 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 uncover the privacy risks associated with an RFID Application ("privacy and data protection impacts") and evaluate 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 Operators on the measures adequate 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. PIA Templates can provide guidance relevant to their industry, sector or application type.

1.1 Purpose

The purpose of the Framework is to provide guidance to RFID Application Operators for conducting PIAs on RFID Applications, as called for in the Recommendation, and to define the common structure and content of the PIA analysis and Reports that result from such PIAs. 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 more efficiently[1]. 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.[2]

The objectives of the RFID Application PIA are to:

- Identify the privacy and data protection implications, if any, of the RFID Application, including whether the RFID Application could be used to monitor an Individual.
- Indicate whether the RFID Application Operator has taken appropriate technical and organisational measures, including establishing controls and measures for Individuals, to ensure the protection of personal data and privacy.
- Document the technical and organisational measures implemented for the appropriate protection of personal data and privacy including measures in place to mitigate identified privacy and data protection impacts.
- Document the overall analysis and result in a PIA Report that can be submitted to the competent authorities, such as data protection authorities, before deployment.

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 Applicability

The Framework identifies the steps of the PIA process and the common elements and structure of PIA Reports to be developed by RFID Application Operators. The Framework may be used directly for PIA Reports and may also be used for the creation of PIA Templates specific to industry sectors, Application types, or other commonalities. Further, the Framework includes mitigation measures to prevent the occurrence of potential threats as defined in the PIA Report or in the Templates, if applicable.

1.3 Key Concepts

There are a number of key concepts used in the Framework that warrant description. ***RFID*** is a technology approach using 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

---

1 The concept of mutual or multiple recognition across entities and sectors for the deployment of previously vetted RFID applications should be explored.

2 Point 5 a) of the European Commission Recommendation of May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification C(2009) 3200 final.

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 supported by back-end systems and networked communication infrastructures, and are operated by one or more ***RFID Application Operators***. If an RFID Application Operator makes determinations related to the processing of personal data, its role would 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.

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

- *A **PIA*** is a process whereby a conscious and systematic effort is made to assess the privacy and data protection impacts of options that may be open in regard to RFID Applications.

- 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.

- ***PIA Reports*** document PIAs based on the Framework. 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.

- ***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 ***User*** and ***Individual,*** are also described in Appendix B: Glossary. Terms from Directive 95/46/EC related to data protection are incorporated by reference.

1.4 Internal Procedures

(a) 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 submit the PIA Report 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 obligations set in the PIA Report.

- *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.

- *Documentation* about when a new or revised PIA Report is warranted. Criteria should include significant changes in the RFID Application, such as material changes in the purposes, types of information processed, uses of the information, or controls employed, defining of a period of regular review or 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.

(b) 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 Section 2.3.7.

1.5 Classification criteria of RFID Applications

When conducting a PIA process based on this Framework, RFID Applications can be classified and assigned a level according to the following criteria:

- **Level 0.** The RFID Application does not process personal data. The RFID Tag Information does not contain personal data and tagged items are intended to be possessed only by the User. The RFID Application does not link RFID Tag Information to personal data.

- **Level 1.** The RFID Application does not process personal data. Tagged items under the RFID Application are intended to be possessed by Individuals. However, the RFID Tag Information does not contain personal data and the RFID Application does not link RFID Tag Information to personal data.

- **Level 2.** The RFID Application processes personal data. The RFID Tag Information does not contain personal data, but the Application links non-personal RFID Tag Information with persons or personal data. Additional considerations may be necessary when the Application processes sensitive personal data (e.g., medical or biometric information).

- **Level 3.** The RFID Application processes personal data and the RFID Tag Information contains personal data. Additional considerations may be necessary when the Application processes sensitive personal data (e.g., medical or biometric information).

The following table summarises how Applications should be categorised according to these levels. The definitions provide the complete guidance. By answering all three questions for an RFID Application, the table shows the relevant level of the given Application. For example, if pallets are tagged, and the tags contain no personal information (1. "No") but the Application links to personal data (2. "Yes"), then the Application should be designated Level 2.

1. Does the Tag contain personal data?	2. Does the RFID Application link to personal data?	3. Are Item level tags intended to be possessed by individuals?	Level
No	No	No	0
No	No	Yes	1
No	Yes		2
Yes			3

2. The PIA Process

To provide for a common approach to the PIA process across the wide range of RFID Applications, the Framework identifies the common elements of PIA Analysis and Reports. The Framework will provide consistency of PIA Reports submitted by RFID Application Operators to the competent authorities and will support the analysis of PIA Reports and of the resolutions reached by the RFID Application Operators.

2.1 Initial Analysis

The very first step of a PIA process is to determine whether a PIA Report is required. To this end, the RFID Application Operator needs to answer the following four questions:

- Does the RFID Application process personal data?
- Does the RFID Tag Information contain personal data?
- Does the RFID Application link RFID Tag Information to personal data?
- Are tagged items intended to be possessed by Individuals?

The RFID Operator will build its initial assessment based on relevant factors outlined in Part A below, with particular attention to points 2.3.3 to 2.3.6, and document the assessment in accordance with internal procedures.

- If the answer to all the above questions is "No", the RFID Application is a "level 0" Application in accordance with Section 1.5 and does not require further analysis or a PIA Report.
- If the answer to at least one of the above questions is "Yes", RFID Applications Operators should proceed by drafting a PIA Report according to the next steps of this Framework.

2.2 PIA Report Structure and Content

As previously noted, the Framework focuses on what is needed to create suitable PIA Reports that reflect the facts about RFID Applications that have privacy and data protection implications. PIA Reports must therefore a) be easy to understand by both technical and non technical audiences, b) be written in a clear and accurate manner and c) provide sufficient information so that the competent authorities can understand the analyses performed by, and have confidence in the actions taken by, the RFID Application Operators.

It should be noted that the levels listed in this Framework in Section 2.3.7 may vary depending on the industry applying particular RFID technology for specific uses. For example, a healthcare Application could potentially encompass a considerably different use of personal data than that of a retail Application. Depending on the nature of the RFID Applications, especially the levels of the RFID Application according to Section 2.3.7, the levels of detail of PIA Reports may vary.

A PIA Report should contain four parts according to this Framework:

- **Part A**. RFID Application Description and Scope
- **Part B**. RFID Application Governing Practices
- **Part C**. Accountability
- **Part D**. Analysis and Resolution.

The following Sections describe the expected content of each of these parts, which together form the PIA Report. However, flexibility in the PIA Report format is allowed to account for RFID Applications with varying levels of privacy and personal data implications. For example, mere checklists may be appropriate for RFID Application Operators using RFID Applications that present low levels of privacy and personal data implications, whereas more robust processes may be necessary for RFID Application Operators dealing with more complex RFID Applications that involve higher levels of privacy and personal data implications. This Framework provides guidance to RFID Application Operators in accordance with the levels assigned to the RFID Applications.

PIA Templates should be developed that keep in mind the different audiences that will need to use or evaluate the Template, including internal operators, reviewers, and approvers, and external stakeholders like competent authorities.

2.3 Part A: RFID Application Description and Scope

The section covers the description of the RFID Application such as setting up the Application, clarity of entities engaged with the Application, Application design, and collection and use of data. This section will help guide the privacy impact assessment process in Sections B-D.

This Section of the PIA Report should provide information about the RFID Application including the core RFID technology, RFID Tags, RFID Readers, read ranges, frequencies as well as back-end systems and communication infrastructure, to the extent that these interface with the processing of information by the RFID Application. It should include facts about the information collected, derived, used, transferred or otherwise processed by the RFID Application, the Individuals (if any) related to the information processed in connection with the RFID Application (whether they are identified, identifiable, or not), and the Users of the information processed by the RFID Application (including other parties who access the information, RFID Application or RFID Tags, or have the information from the RFID Tags transferred to them).

The objective is to describe the RFID Application, including the business context in which it will operate. Special attention should be placed on the RFID Application's purpose and the flow of information among its components and with other parties. Particular attention should be paid to:

- Whether the information in RFID Tags contains personal data as defined in Directive 95/46/EC.
- Whether the information in RFID Tags may be linked to personal data to which the RFID Application Operator or other User has access.
- The scale of the RFID Application (local, national, European, international).

2.3.1 RFID Application Operator

In the PIA Report, the **RFID Application Operator** should be identified, and should include the following information:

- Legal entity name(s).
- Primary function(s) (i.e., related to the RFID Application).
- Location(s) (e.g., headquarters of the RFID Application Operator).
- Point(s) of contact with contact information.

2.3.2 Other Parties and Users of the RFID Application

Other legal entities providing processing on behalf of the RFID Application Operator, or operating as joint RFID Application Operators, should also be identified and described in the same manner. The PIA Report should include the following information that is relevant to the RFID Application:

- Legal entity name(s).
- Primary function(s) (i.e., related to the RFID Application).
- Location(s) (e.g., Headquarters).
- Point(s) of contact with contact information.

The PIA Report should also describe the types of **Users** of the RFID Application. The items noted here will vary depending on the industry sector(s) in which the RFID Application is applied.

2.3.3 RFID Application Description

Next, the **RFID Application** should be described. For that purpose, the following information should be included:

- RFID Application name.
- Purpose(s), including specific uses of the RFID technology as part of the RFID Application, and indicating the benefits of using RFID as compared with non-RFID methods (if applicable).
- RFID Application description, including a description of the technology used (e.g., the core RFID technology, RFID Tags, RFID Readers, read ranges or read frequencies).
- Indication of the geographical scope of the RFID Application.
- Type of information processed.
- Stage of development of the RFID Application and planned deployment date.

2.3.4 Individuals and Users Interacting with the RFID Application

The PIA Report should identify the types of **Individuals** interacting or otherwise involved with the RFID Application and whether the location of Individuals or Users will be monitored through the RFID Application.

It should consider the following types of Individuals and whether they are identified, identifiable, or not, and if identified or identifiable to what level (e.g., name, identification number, pseudonym, location, home address):

- Individual.
- Household.
- Person who possesses an RFID Tag (e.g., on an item owned or otherwise possessed).

2.3.5 Presence of Personal Data in the RFID Application

The PIA Report should indicate if the RFID Application processes personal data, in accordance with the definition contained in Directive 95/46/EC, and the basis for the processing under the Directive if applicable. The Report should document efforts to design the Application so as to lawfully process the minimum amount of personal data that is necessary and proportionate. The RFID Application Operator should also specify the purpose for which personal data is processed by the RFID Application.

The RFID Application under review should consider whether any of the following categories of personal data are applicable (listed in alphabetical order and not intended to be exhaustive):

- Behavioural
- Biometric*
- Contact information
- Criminal history
- Demographic
- Education and other credentials
- Employment-related
- Family or social network
- Financial
- Genetic*
- Health*

- Lifestyle
- Personal communications
- Photographs or video
- Political opinions*
- Racial or ethnic origin*
- Religious beliefs*
- Sexual life*
- Transactions and purchases
- Vehicle identification

– *For each category of personal data involved*, the PIA Report should indicate whether the information in the RFID Tag alone or in the RFID Application as a whole is identified, identifiable, or not, to an Individual, a product instance, or some other object in the RFID Application.

– *For each category of personal data identified*, an indication as to the source of the information in the RFID Application as a whole or in the RFID Tag alone should be included. For example, it should be noted if the information is assigned by the RFID Application, provided by the RFID Application Operator or by another party, derived by the RFID Application, or otherwise provided by an Individual or User. The means and methods used to collect or derive the information should be identified as well.

Once it has been determined that personal data is processed by the RFID Application, the nature of the processing should be indicated in the PIA Report as follows:

- The categories of personal data that could potentially be processed by the RFID Application.
- The categories of personal data stored in RFID Tags related to the RFID Application.

Special attention should be paid to the processing of sensitive personal data, as starred above, which is only allowed under the strict conditions of Directive 95/46/EC and implementing national legislation.

2.3.6 RFID Application Data Flows

The PIA Report should provide a chart of the data flows of personal data or of other information that will be associated with personal data in the RFID Application and other directly related Applications. The chart should, in particular, show whether personal data processed by the RFID Application, if any, is linked to other information processing systems within the RFID Application Operator’s organisation or other Users. This will allow the RFID Application Operator to determine the applicability of further subparts of the Framework.

2.3.7 RFID Application Classification

On the basis of the information provided in Sections 2.3.1 to 2.3.6., the PIA Report should identify the level of the RFID Application according to the classification provided in Section 1.5.

Based on the overall description of the Application, the assignment of levels to the RFID Application will help to place particular attention on specific subparts of the PIA Report. The level of detail involved in the PIA Report may increase with each particular level depending on the particulars of the RFID Application.

2.4 Part B: RFID Application Governing Practices

Given the description of the Application and the nature of data processing in Part A, Part B is designed to address data protection, privacy, and security features built into the Application to minimize potential risks related to the deployment of the Application. These mitigation measures address management practices by the RFID Application Operator, access by authorised or unauthorised parties, lawful processing of personal information, security features, internal and external data transfers, and individual access and control rights. The PIA Report or Template may provide further detail regarding governing practices relevant to their industry or Application.

The practices described in this part are ancillary to the existing European Union data protection regulatory framework and are not intended to replace it or modify its scope. The completion of this part (together with Part C) will enable an RFID Application Operator to assess whether an RFID Application involves privacy implications and Part D will help determine whether those implications are mitigated when considering the governing practices and other controls in place.

Part B applies to an RFID Application classified as either Level 1, Level 2, or Level 3, irrespective of whether the RFID Application processes personal data or not. The determination about whether personal data are processed or not by the RFID Application is made in accordance with Part A, in which the RFID Application is described. The level assigned to the RFID Application is relevant, as the amount of detail needed to complete this part will depend on the level referred to in Section 2.3.7.

This part of the PIA Report should be used to document facts about: (a) the features and controls in place to protect and govern the use of the RFID Application; (b) the components of the RFID Application, such as RFID Tags and back-end systems; and (c) the associated information processed in the RFID Application, with particular emphasis on achieving appropriate levels of privacy and the protection of personal data based on a risk management approach. If any of the components of the RFID Application adhere to a specific set of established privacy and data protection standards or guidelines, that fact should also be indicated as part of the PIA Report.

2.4.1 Individual Access and Control

(a) **Individual Access**

The PIA Report should describe the RFID Application Operator's policies on access to information processed by the RFID Application related to personal data, such as:

- Confirmation as to whether personal data are processed,

- The purposes of the processing and the categories of personal data involved,
- Recipients to whom personal data are disclosed, and the right to object to the processing of personal data or withdraw consent, and
- Rectification or erasure of incomplete or inaccurate personal data. (See Section 2.5.2. of the PIA Framework).

(b) **Individual Control**

While conducting PIAs, RFID Application Operators should consider the measures of Individual control relevant to the RFID Applications. Classifying the RFID Applications at the appropriate levels will help RFID Application Operators determine the specific Individual controls needed.

In the PIA Report, RFID Application Operators should evaluate Parts A, B, and C of the Framework to determine whether RFID Tags provided to Individuals represent a likely privacy implication or negatively affect the protection of personal data, and should document in the Resolution section (Part D) the controls instituted and the actions Individuals can take to mitigate these impacts (if any).

Depending on the PIA analysis of the likely threat to privacy or protection of data, for RFD Application Operators in Retail, 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.

2.4.2 System Protection

System Protection (for the back-end systems and communication infrastructure in so far as they are relevant to the RFID Application), with respect to the appropriate protection of privacy and personal data, should also be documented in this Section of the PIA Report. For complex systems at higher levels according to Section 2.3.7, this Section should be decomposed individually to address major components. The following components should be addressed:

- Description of relevant information security policies and procedures, including any references to information security standards or guidelines.
- Access controls related to the type of personal data and functionality of the systems.
- Controls in place to prevent identification if data are personally identifiable but not identified.
- Confidentiality of the personal data in the systems and in the communication infrastructure.
- Retention and disposal of the personal data.

2.4.3 RFID Tag Protection

RFID Tag Protection controls related to privacy and personal data should be indicated in this Section. Facts about the following should be addressed if they are required or otherwise warranted for the RFID Tag itself. This Section is particularly relevant to RFID Applications that use RFID Tags containing personal data, and therefore additional or different measures may need to be observed.

Based on a risk management approach in regard to the protection of personal data, such protection may not be required or warranted if the RFID Tag is not possessed by an Individual and does not involve the linkage of personal data. These protection controls include the following:

- Access control to functionality and information, including authentication of readers, writers, and underlying processes, and authorization to act upon the RFID Tag.
- Confidentiality of the information (e.g., through encryption of the full RFID Tag or of selective fields).
- 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.

2.4.4 Access and Transfers to Other Parties

The PIA Report should address the transfer and access by other parties and Users of the personal data processed by the RFID Application. The following components should be considered and documented in the PIA Report:

- Name or type of other party (-ies).
- Location of other party (-ies) identified in Section 2.3.2 to whom the information is transferred or from where information is accessed.
- Method(s) of transfer or access.
- Purpose(s) for transfer or access.

2.4.5 Adequacy of Transfers Outside the European Economic Area (EEA)

This Section should indicate the legal framework serving as the basis for the transfer of personal data processed by the RFID Application. This may include, for example, contractual clauses, determinations of the adequacy of data protection laws, consent, and other techniques to legitimise the access or transfer.

2.5 Part C: Accountability

Again, given the description of the Application and the nature of data processing in Part A, Part C is designed to address data protection, privacy, and security features related to the Application to minimize potential risks linked to the deployment of the Application, in the area of accountability. This section is intended to address external awareness regarding RFID Applications, and to support overall accountability and compliance by the RFID Application Operator with the PIA Report and other requirements that may apply. The PIA Report or Template may provide further detail regarding accountability issues relevant to their industry or application.

This Section of the PIA Report should address the business operations and regulatory compliance processes managed by the RFID Application Operator. It should describe how Individuals are notified about use of an RFID Application, and how they may interact with the RFID Application Operator regarding the RFID Application.

2.5.1 Transparency and information

2.5.1.1 Published Information Policy

The PIA Report should describe the information policy provided regarding the RFID Application. More specifically, it should indicate if the information policy includes the following elements:

- Identity and address of the RFID Application Operator.
- Purpose of the RFID Application.
- Data processed by the RFID Application, in particular if personal data are processed, and whether the locations of RFID Tags will be monitored.
- Likely privacy and data protection impacts, if any, relating to the use of RFID Tags in the RFID Application and the measures that Individuals can take to mitigate these impacts.

2.5.1.2 Notice

The PIA Report should indicate how Individuals are notified in a concise, accurate and easy to understand manner, of the presence of RFID Readers, the identity of the RFID Application Operator, and a point of contact for Individuals to obtain the information policy. For RFID Applications used in the retail trade sector, the PIA Report should also indicate how Individuals are notified of the presence of RFID Tags placed on or embedded in products.

2.5.1.3 Other Stakeholders

A summary of the PIA Report or information on the initial analysis should be made available to the relevant stakeholders or its representatives interacting or otherwise involved by the RFID Application, in accordance with applicable law.

2.5.2 Redress Methods

The PIA Report should describe the following **Redress Methods,** and if and how they 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).
- 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.

2.5.3 Regulatory Compliance

In addition, **Regulatory Compliance** specific to the industry and Member State(s) in which the RFID Application will be used, should be indicated in this Section. For example, the RFID Operator should verify that the RFID Application is compliant with Directive 95/46/EC and Directive 2009/136/EC if applicable.

2.5.4 PIA Report Initiation and Updates

The PIA Report should indicate whether this is a new or revised PIA, along with any changes made from prior PIAs, in accordance with internal procedures documented in Section 1.4.

2.6 Part D: Analysis and Resolution

This Section of the PIA Report should indicate the business, compliance, or legal determinations made regarding the RFID Application. The facts entered about the RFID Application in Parts A, B, and C should be considered to make a determination as to the overall privacy impact and compliance of the RFID Application.

The **RFID Application Operator** should use the categories below to indicate the privacy and data protection implications of the RFID Application:

- **Ready for deployment**. The RFID Application as described and possibly mitigated provides for suitable practices, controls, and accountability.

- **Not ready for deployment**. The RFID Application is not approved for operations in its current state. A specific corrective action plan will be developed, and a new privacy impact assessment will be performed and documented to determine if the Application has reached an approvable state.

RFID Applications with high levels of privacy and personal data implications, and which are lacking adequate controls and protections, should be rated as "not ready for deployment."

The resolution (i.e., whether the RFID Application is ready for deployment or not ready for deployment and, if ready for deployment, at what level it operates) should be associated with the following information:

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

The internal approval process, including criteria such as next steps, timing, and required signatures, should be documented in the Internal Procedures described in Section 1.4.

The signed PIA Report that contains an approved resolution, excluding proprietary information not pertinent to the PIA, should be made available to the competent authority at least 6 weeks before deployment. 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 Artice 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 Section 1.4 (b) of the PIA Framework.

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

- "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

- "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

- "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 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," Official Journal of the European Union, 13 April 2006, L 105/54, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063: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

- "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

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:

Deactivation. Any process that stops interactions of an RFID Tag with its environment which does not require the active involvement of the consumer.

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.

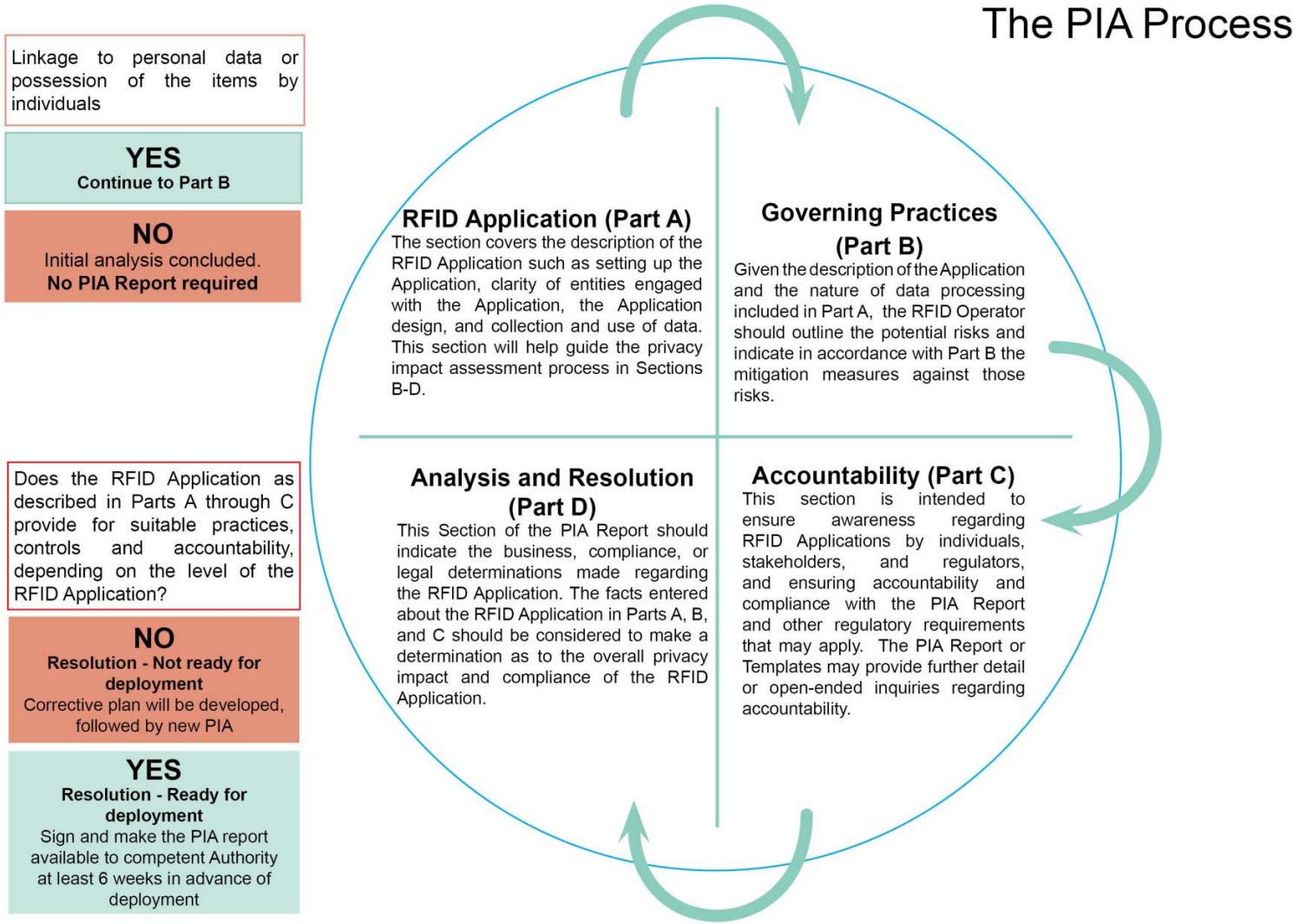
RFID Reader. A fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.

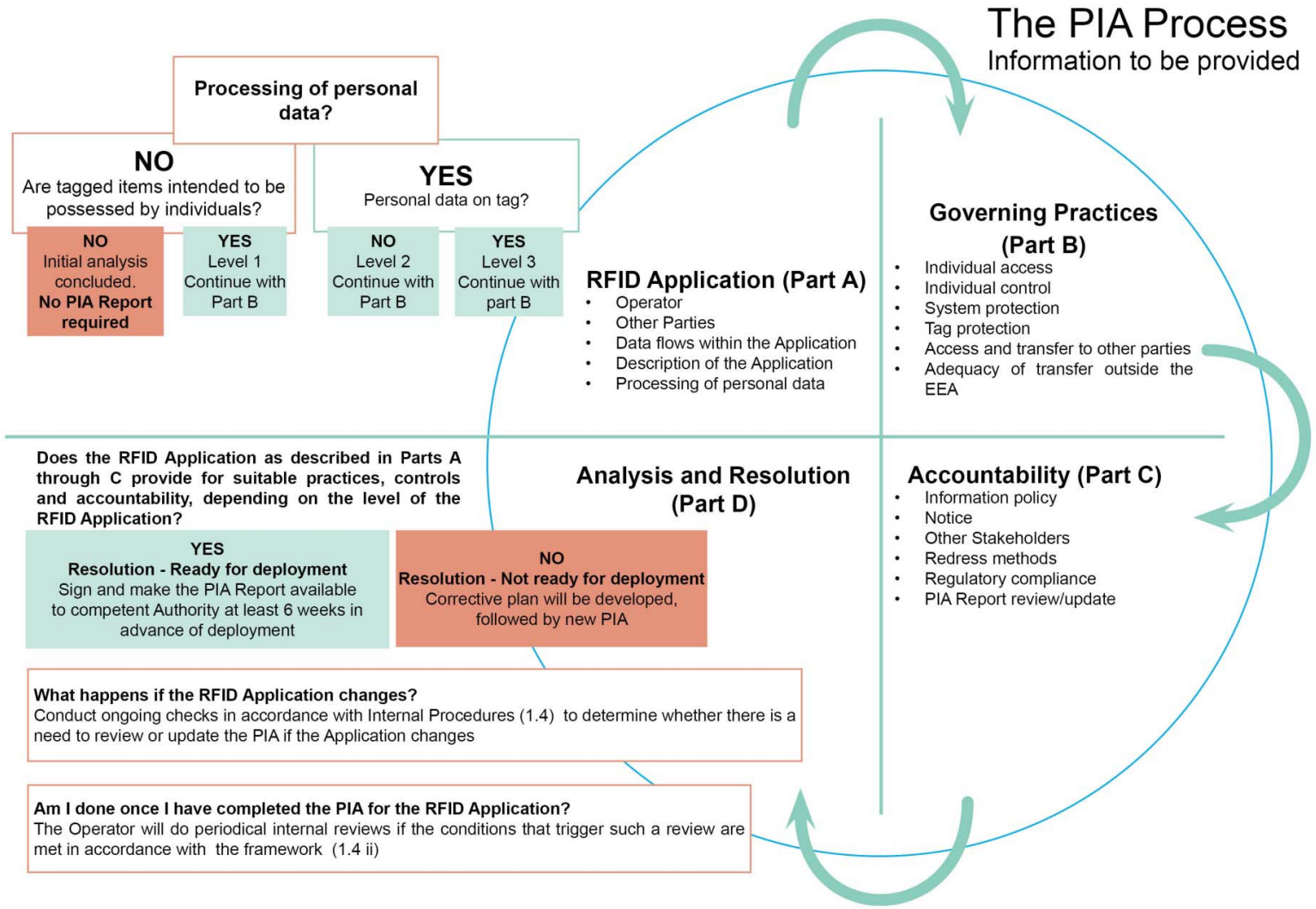
RFID Tag. Either a RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer.

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.

Appendix C: The PIA Process




The PIA Process
Information to be provided
Processing of personal data?
NO
Are tagged items intended to be possessed by individuals?
YES
Personal data on tag?
NO
Initial analysis concluded.
No PIA Report required
YES
Level 1
Continue with Part B
NO
Level 2
Continue with Part B
YES
Level 3
Continue with part B
RFID Application (Part A)
Operator
Other Parties
Data flows within the Application
Description of the Application
Processing of personal data
Governing Practices (Part B)
Individual access
Individual control
System protection
Tag protection
Access and transfer to other parties
Adequacy of transfer outside the EEA
Does the RFID Application as described in Parts A through C provide for suitable practices, controls and accountability, depending on the level of the RFID Application?
Analysis and Resolution (Part D)
Accountability (Part C)
Information policy
Notice
Other Stakeholders
Redress methods
Regulatory compliance
PIA Report review/update
YES
Resolution - Ready for deployment
Sign and make the PIA Report available to competent Authority at least 6 weeks in advance of deployment
NO
Resolution - Not ready for deployment
Corrective plan will be developed, followed by new PIA
What happens if the RFID Application changes?
Conduct ongoing checks in accordance with Internal Procedures (1.4) to determine whether there is a need to review or update the PIA if the Application changes
Am I done once I have completed the PIA for the RFID Application?
The Operator will do periodical internal reviews if the conditions that trigger such a review are met in accordance with the framework (1.4 ii)