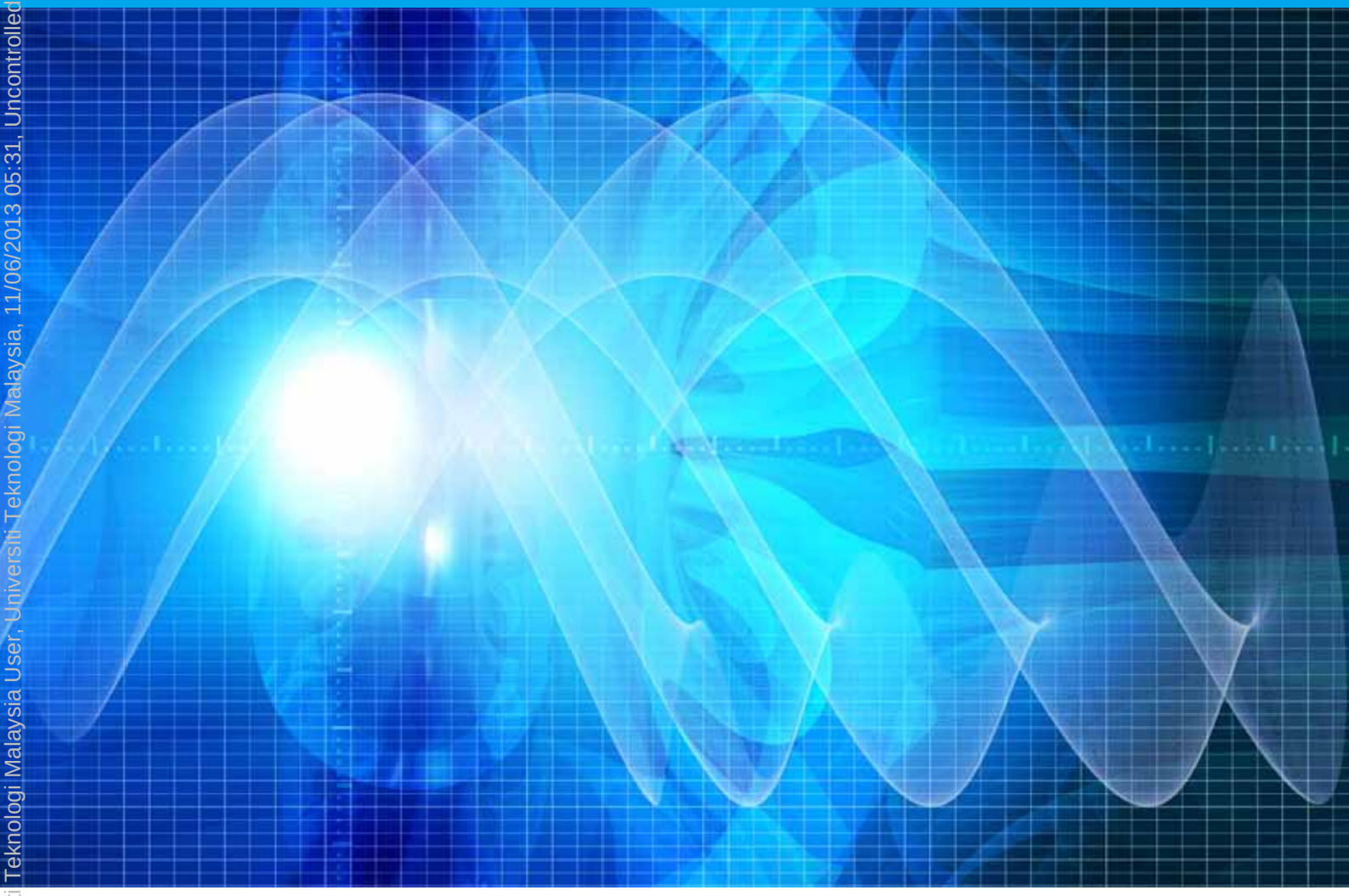
PAS 94:2013

Implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) applications – Guide



Department for Business Innovation & Skills

bsi.

Publishing and copyright information

ISBN 978 0 580 76452 3

ICS 33.060.99, 47.020.70, 33.040.40

Publication history

First published May 2013

Contents

Foreword

This PAS was commissioned by the UK Department for Business, Innovation & Skills (BIS). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came in to effect on 31 May 2013.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the Steering Group:

- Avery Dennison
- BSI Consumer & Public Interest Network
- Chartered Institution of Logistics and Transport
- Department for Business, Innovation & Skills
- GS1 UK
- London School of Economics
- Marks and Spencer

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS may be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a guide, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in italic type, and does not constitute a normative element.

Spelling conforms to The Shorter Oxford English Dictionary. If a word has more than one spelling, the first spelling in the dictionary is used.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

0.1 Background to RFID and data/privacy protection (DPP)

Radio frequency identification RFID tags in devices such as mobile phones, computers, fridges, books and cars bring many potential advantages for businesses, public services and consumer products.

Examples include improving product reliability, energy efficiency and recycling processes, paying road tolls without having to stop at toll booths, cutting time spent waiting for luggage at the airport and lowering the environmental footprint of products and services.

Similarly, many hospitals use RFID tags to track inventory and identify patients. While this technology can improve the overall quality of healthcare, the benefits should be balanced with privacy and security concerns.

The use of RFID systems can potentially create privacy, security and data protection risks.

Personal data might be read from RFID tags without the permission of the individual concerned. Even where personal data is appropriately obtained, risk can develop through insecure storage.

An emerging challenge is that of scale. McKinsey Global Institute (MGI) (May 2011) has noted that the amount of data being captured by organizations is growing exponentially, and analysing large data sets (so called "big data") will become a key driver of competition and economic growth.

Big data typically creates value by establishing and analysing relationships between many different pieces of data. Some of this data will be personal in nature, and individual privacy could be endangered by this process of data mining, e.g. associating an individual with the real time location data from their car, mobile phone and transport card.

Whilst the scenario of pervasive data collection is a recent phenomenon, the underlying issues of protection of data and personal privacy are not.

It is important that any organization considering the installation of a RFID system appreciates that the system should be compliant with existing data and personal privacy protection legislation.

In 2008, the European Commission issued a standardization mandate 436 [1] to the European standardization organizations CEN, CENELEC and ETSI in the field of information and communication technologies applied to RFID systems. The mandate addressed data protection, privacy and information security aspects of RFID. In response to this mandate, European Standards on the privacy impact assessment (PIA) process for use in RFID applications and on the public notification signage associated with RFID applications will be published in 2014.

0.2 Purpose of this PAS

This PAS acts as a bridging document until the European Standards are published, and is also intended to stimulate input to the public enquiry stage of the European Standards which will take place between March 2013 and July 2013. This input will be channelled through the secretariat of the relevant BSI technical committee IST/34, Automatic identification and data capture techniques.

The guidance is designed to help an organization achieve and maintain compliance with existing national legislation on data and personal privacy protection.

This page deliberately left blank.

1 Scope

This PAS gives guidance on implementing privacy impact assessment (PIA) frameworks in radio frequency identification (RFID) applications. It explains:

a) how to carry out a PIA to:
   i) evaluate potential risks to personal privacy;
   ii) mitigate these risks;
   iii) record any residual risk;
b) how to design and place signage to notify the public that:
   i) they are entering an area where RFID readers might be operating;
   ii) an item is carrying a RFID tag.

Together with the public notification sign, the PIA process provides a common approach within the European Union (EU) to achieve compliance with public privacy and data protection principles.

The RFID application operator is responsible for carrying out the PIA process.

This PAS is relevant where RFID readers are located in spaces where the public might have access, and/or where items carrying RFID tags might pass through areas to which the public might have access.

This PAS is intended for use by general managers and by ICT specialists in all economic sectors and all sizes of organization, and is written in the context of the introduction of the RFID PIA methodology within Europe.

This PAS is applicable to all public and private organizations within the EU operating, or considering the implementation of, a RFID system.

2 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

2.1 individual

natural person who interacts with or is otherwise involved with one or more components of a RFID application (e.g. back-end system, communications infrastructure, RFID tag), but who does not operate a RFID application or exercise one of its functions.

2.2 information security

preservation of the confidentiality, integrity and availability of information

2.3 monitor

carrying out an activity for the purpose of detecting, observing, copying or recording the location, movement, activities, or state of an individual

2.4 personal data

information relating to an identified or identifiable natural person ("data subject")

NOTE *An identifiable natural 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*

2.5 radio frequency identification (RFID)

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

2.6 RFID application

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

2.7 RFID application operator

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 a RFID application

2.8 RFID reader

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

2.9 RFID tag or "tag"

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

2.10 RFID tag information or information on the RFID tag

information contained in a RFID tag and transmitted when the RFID tag is queried by a RFID reader

2.11 user

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

3 The PIA process

3.1 General

As with any systems change, the implementation of a RFID application can introduce new risks as well as benefits.

Many of these risks can be related to internal processes, with the required mitigation being obvious, and the measurement of success in eliminating potential risk also only being reported internally.

The risks in relation to data protection and in particular privacy can be less easy to establish, and use of a formal risk assessment procedure will assist in achieving compliance with relevant data/privacy protection (DPP) legislation and in preparing the summary PIA report.

The PIA process outlined in this clause takes the general principles of risk management and applies these to a generic RFID application. It is intended that this framework should be adapted by application sectors to meet their specific business needs.

More detailed legal information can be sourced from the Information Commissioner's Office.

It is the responsibility of the RFID application operator to carry out the PIA process. This can be done at any time, but it is especially relevant when a system is being designed or when changes are made.

During this process, careful consideration should be given to the distinction between data protection and personal privacy, and the different methods of mitigation required.

- Data protection is required from the instant data is captured (in this case by RFID readers, but the concept is applicable to all automatic data capture techniques) until it is deleted from the operators system.
- Personal privacy has to be protected at all times and in all places, even when the individual is outside the immediate area where RFID data could be collected by the operator's system.

A more detailed overview of automatic identification and privacy is given in Annex A.

3.2 Outline

The PIA process is a multi-stage process which requires the RFID application operator to describe the scope and purpose of the RFID application. It includes the following:

1) Describe application, including:
   a) users and other personnel interacting with the application;
   b) presence or otherwise of personal data in the system;
   c) what data is captured and stored.
2) Identify, record and quantify potential risks to personal privacy from the operation of the RFID application. Consider:
   a) tag removal/deactivation (typically retail sector only) (see **3.9**);
   b) protection mechanisms for tag data and overall system;
   c) data access, including flows outside the EU.
3) Document current and proposed technical and organizational controls to mitigate identified risks.
4) Document the results of the analysis regarding the application, including:
   a) the business, compliance and legal determinations from the process;
   b) the overall impact on privacy;
   c) whether the application is approved for deployment.

A completed PIA report should typically include:

a) a description of the RFID application as outlined in Annex B;
b) documentation of the four steps outlined above.

An assessment should be carried out by the operator in regard to the privacy protection capability of the readers and tags deployed in the system. This information can be obtained from, amongst other sources, the system integrator and/or reader/tag manufacturer.

3.3 Description of the application

The description of the application should give a comprehensive and full picture of the application, its environment and its system boundaries. The application design, its adjacent interfaces with other systems and information flows should also be described.

Data flow diagrams that show processing of primary and secondary data are recommended to visualize information flows.

Data structures should be documented, so that potential links can be analysed.

Annex B contains a full summary of the elements which can be used to describe a RFID application for the purposes of conducting a PIA.

In addition, the inclusion of information related to the application's operational and strategic environment is recommended. This might include:

- the immediate and longer-term mission of the application;
- identification of stakeholders in the information collected;
- functional requirements;
- potential users;
- a description of the RFID application's architecture and data flows (in particular, interfaces to external systems that might process personal data).

3.4 Initial analysis phase

The RFID application operator should determine whether a PIA of its RFID application is required, and if so, whether a full- or small-scale PIA is warranted.

The RFID application operator should use the decision tree in Figure 1 to help determine whether, and to what extent, a PIA is needed for the RFID application under consideration.

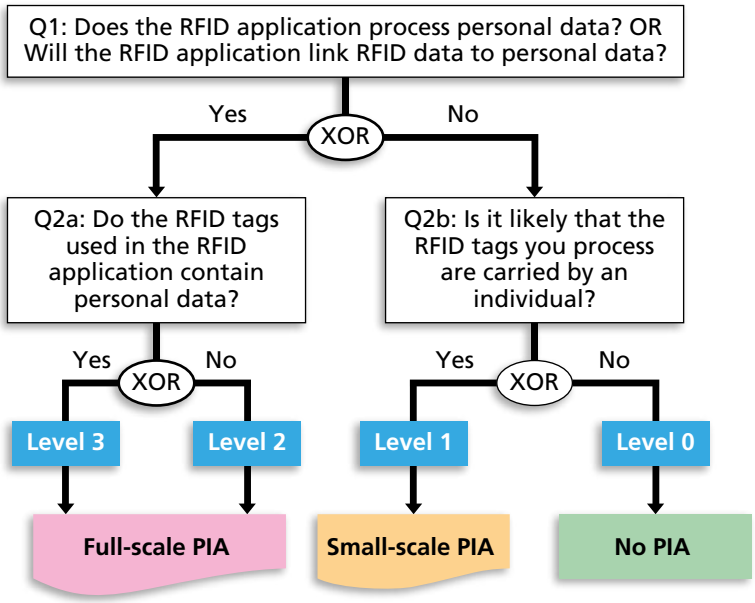
NOTE 1 *In general, if the tags used by the application do not come into possession of people, then the risk category is level 0 and no further work is needed.*

NOTE 2 *A clear understanding of tag and application data for both direct personal data and potentially indirect personal identification is necessary to obtain an accurate interpretation of the decision tree.*

The initial analysis phase determines the level of detail necessary in the risk assessment and therefore whether a full- or small-scale PIA process is required.

This initial analysis should be documented and made available to data protection authorities upon request.

Figure 1 – Decision tree on whether and at what level of detail to conduct a PIA



3.5 Full-scale PIA process

If the initial analysis phase indicates that the application is level 2 or level 3, then a full-scale PIA should be undertaken to ensure that any risk to personal data is both understood and subsequently controlled by appropriate mitigation procedures.

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 might have controls to protect back-end data; or
- level 3 applications might have controls to protect both back-end data and tag data.

RFID application operators should also consider whether the data held in the RFID tag memory 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. In this case a new PIA analysis might be necessary, and/or further mitigating controls might need to be employed.

3.6 Small-scale PIA process

Small-scale PIAs are relevant for level 1 applications, and follow essentially the same process as full-scale PIAs. 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. The required controls and corresponding documentation in the PIA report can be simpler.

3.7 Risk assessment phase

The risk assessment process should consider the risks of a RFID application in terms of:

- likelihood of occurrence;
- magnitude of consequences.

To save time and cost, it is recommended that this risk assessment phase is completed well before final decisions on a RFID application's architecture are taken.

This will allow technical privacy mitigation strategies to be embedded into the system's design, and not 'bolted on' later.

RFID application operators are advised to use the privacy objectives of the EU DPP Directive as a starting point for their risk assessment (see Annex B).

3.8 Identification of risks

Risks can be related to:

- the RFID application components;
- operation of the application (collection, storage and processing infrastructure);
- the data sharing and processing environment in which the application is embedded.

A RFID application operator should consider, on a reasonable basis, the likelihood of a risk to privacy as a result of the operation of the RFID application concerned. Such risks can stem from processes inside or outside the application.

These risks can 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 evaluation of the applicable risks from a privacy perspective; the RFID operator should consider:

- the parties who would be affected by the risk including at least the application operator, individuals in possession of tagged items and users of the application;
- the significance of a risk;
- the likelihood of its occurrence;
- the magnitude of the impact should the risk occur.

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

Annex B provides a detailed list of potential risks.

3.9 Deactivation of tags

A potential concern is the risk that data contained in a RFID tag memory could be used for the profiling and/or tracking of individuals, especially by linking the chip ID to an individual.

It has been argued that retailers who pass RFID tags on to customers, without automatically deactivating or removing them at the checkout, could unintentionally create this risk.

The EC RFID recommendation [2] (see Annex C) requires retailers to deactivate or remove any tags used in their application at the point of sale, 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 used in a retail application, and which 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.

3.10 Identification and recommendation of controls

Controls can be either of a technical or non-technical nature.

- Technical controls are incorporated into the application through architectural choices or technically enforceable policies, e.g. default settings, authentication mechanisms, and encryption methods.
- Non-technical controls are management and operational controls.

Controls can also be categorized as being preventive or detective. The former inhibit violation attempts and the latter warn of violations or attempted violations.

The scanning environment can also create "natural" controls. 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 limited risk.

The identified risks and their associated risk levels should guide the decision on which of the identified controls are relevant and thus should 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 B.

3.11 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.

A 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 a 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 PIA 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.

3.12 PIA report

RFID operators should be aware that the PIA process itself is for internal use and the contents are at least organization-confidential.

In some circumstances, the PIA report might contain sensitive information that has security implications and/or proprietary information of the organization related to products and processes.

The signed PIA report that contains an approved resolution should be given to the assigned organization's data privacy/security official in accordance with the RFID application operator's internal procedures.

This report should be provided without prejudice to the obligations set forth in the Directive 95/46/EC [3] for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC [3].

4 The common European RFID notification signage system

4.1 General

Clause 22 of the EC recommendation [2] calls for increased awareness by individuals and organizations about the features and capabilities of RFID, and for mitigation of the associated risks for privacy.

The primary methodology for mitigation of risk to data protection and privacy is the PIA process. This is a risk assessment process required to be undertaken during the design and implementation of RFID applications that might handle data deemed to be of a personal nature.

The common RFID notification signage system is a key mitigating solution where the PIA indicates there is risk to the individual.

The notification signage system described in **4.2** is modelled on the well-established, and publicly accepted, notification signage system used for CCTV systems in the EU. The signs resulting from application of the system are seen widely and are easily recognized by the individual.

Case studies for the use of RFID notification signage are given in Annex D.

4.2 Definition of the common European notification signage system

This definition should be read in the context of the completion of a PIA of the RFID application, which indicates the need for public notification signage to be implemented. The PIA process will define the identity of the data controller.

The common European RFID notification sign consists of three elements:

- a graphic emblem derived from the generic emblem defined in BS ISO/IEC 29160;
- a textual description of the purpose of the RFID application being notified, together with the legal name of the RFID application operator and their telephone number (normally that of the designated data controller);
- a textual definition of the contact point from which further information may be obtained about the application, including, among other things, the information policy of the operator. The contact point may be defined by any of the following methods: postal address, e-mail address, telephone number, webpage URL.

It is recognized that the signage system will be applied in a very wide range of circumstances, and with potential constraints in terms of available space, printing technique, etc. The signage system is therefore generally non-prescriptive in relation to design, font, colour, etc., in order that the signage can be printed with minimum changes in process.

The notification sign should be regarded as belonging to the general set of EU trade regulation signs such as weights and measures, CE marks, etc. The sign should therefore conform to the norms of visibility, legibility and accessibility as applied in the relevant member states.

The notification sign should not be regarded as a hazard sign, and the sign should not utilize shapes/outlines and/or colours that might imply danger.

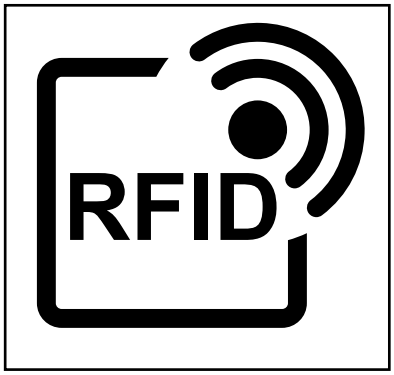
It is recognized that the operator, especially in the case of small organizations, buying groups, franchises, etc. may delegate the contact point task to third parties such as call centres. However, this does not reduce the legal responsibilities of the operator in terms of compliance with data protection and privacy regulations.

4.3 The common RFID emblem

The use of the common European RFID emblem is mandatory on all RFID notification signs, and is designed to permit quick and easy recognition by individuals of the presence of RFID systems in public areas such as shops, public transport locations or libraries or directly embedded in products.

The common RFID emblem for Europe will be the generic version of the BS ISO/IEC 29160 RFID emblem published by the International Standards Organization.

Figure 2 – Generic BS ISO/IEC 29160 RFID emblem



NOTE 1 *A reversed image is also available.*

ISO/IEC 29160 is in process of being adopted as a European Standard (EN): this will allow it to be referenced by the forthcoming signage standards due in 2013/14. EN ISO/IEC 29160 will provide specific informative content regarding use of the notification signage within Europe.

In particular it provides clarification regarding the minimum size of the emblem. When used as part of a RFID notification sign, the requirement is that it should be of sufficient size to be legible at the normal reading distance for the sign.

The RFID notification sign sits within the overall set of signage required by trading standards, and these standards generally specify the meaning of legibility, and also accessibility of individuals with impaired vision.

The reasons for selection of the generic BS ISO/IEC 29160 emblem include:

- distinctiveness, with RFID text to reinforce message;
- ease of printing on any type of printer;
- preprint or on-demand printing;
- scalable for large or small signs;
- global standard;
- non proprietary.

NOTE 2 *Some concerns have been expressed about the emblem by various stakeholders.*

- *It is seen as a European emblem rather than a global emblem, and global organizations do not want to have to label products especially for Europe: in fact, products sold in Europe already have to conform to a range of specific EU labelling regulations, so there should be no adverse impact on SKU holdings.*
- *Some organizations have asked for the GS1 logo to be used on the basis that this is global. The GS1 logo, in common with a number of other logos:*
  - *is proprietary and may not be used or available to organizations who are not of GS1;*
  - *has system operability and data structure implications beyond simple notification.*

4.4 Purpose of the application

The scope and purpose of the application(s) should be described on the sign, for example:

- RFID systems operate in this area for reasons of inventory control and product security;
- RFID systems operate in this area for control of tickets;
- RFID systems operate in this area to improve availability of lending items.

The wording is at the discretion of the operator.

It is recommended that the description is in general terminology in order to reduce the need for new signs in the event of changes in the operation of the application.

Where an operator is operating several different applications in the same area, then each of these applications should be listed in the scope and purpose element of the sign.

4.5 Contact point

The contact point element of the sign should provide the individual with:

- name of the operator of the application;
- at least one method of contact available to the general public.

This information should be displayed in human readable text. Additionally, machine readable methods such as a quick response (QR) code may be used.

4.6 Name of the operator of the application

Only one RFID application operator's name and identifier should be displayed on any particular common European RFID notification sign.

It is important to understand that a sign displayed by one operator does not apply to other operators in the same area, even if their application is identical. Each operator's name and contact point should be specified together with the scope and purpose of the application. It is recommended that the operator's

details are placed on separate physical signs to avoid a need to replace or revise the whole sign when one operator needs to change their text.

An example of this might be a transport hub such as a train station, bus station or airport.

NOTE *In this situation, where there might be a number of train operators using a train station, the number of signs could be minimized if a third party such as the train station operator or a train operators' trade association would provide a single point of contact for individuals seeking further information about the several RFID applications deployed within the station. This would simplify communications for both operator and individual, and minimize the cost associated with changes of operator. However, it should be understood that such an arrangement does not change the basic legal responsibilities of the individual operators: only the communications aspect of the signage is being delegated.*

The application operator's name displayed should be the name of an EU registered company.

An EU company identifier may supplement the RFID operator's name but cannot replace it. A company identifier should be presented on the same row and follow the operator's name.

No other information in any form should be present on the same row as the RFID application operator's name or company identifier.

4.7 Contact method

The contact point element of the sign should provide at least one method of direct contact generally available to the individual. This may include postal address, e-mail address and telephone number.

Where a telephone number is provided, this should be accessible during normal business hours as a minimum.

Additionally, indirect methods such as websites may be used: these should contain a direct method of contact with the application operator.

The contact point should also give the name and position of the person in charge of the application.

It is recognized that the operator, especially in the case of small organizations, buying groups, franchises, etc. may delegate the contact point task to third parties such as call centres. However, this does not reduce the legal responsibilities of the operator in terms of compliance with data protection and privacy regulations.

4.8 Placement of common European RFID notification signs

The EC recommendation [2] defines two situations where signage is required:

- where RFID readers are present;
- where tags are attached to, or embedded in, items such as retail products, library items, contactless transport tickets and contactless bank cards.

RFID application operators should be aware that there is an important legal, as well as practical, difference between the two situations.

In the case of areas where readers are known to be located and the operator notifies the public of their presence, the primary concern is one of data protection, i.e. that the capture, transfer, storage and access of any data in the RFID application is handled by the RFID application operator in compliance with the relevant legislation.

In the case of tagged items, the main concern is one of personal privacy, since a tag on or inside an item carried by an individual could potentially be read anywhere at any time. The reader system might be:

- properly notified within an area, but the individual might not wish to allow the presence of the tagged item to be detected;
- a component of a consumer device such as a mobile phone, where such notification would be impractical;
- an illegally operated device.

In order that the individual can be given the option to prevent a tag being read, they should first be advised of the presence of the tag. It is for this reason that a common notification sign should be placed on a tagged item. The possible constraints on size and also print definition of the notification sign are recognized in this PAS and the future signage EN.

4.9 Presence of readers

4.9.1 General

Clause 8 of the EC recommendation [2] notes that *"Member States should ensure that operators take steps to inform individuals of the presence of readers on the basis of a common European sign, developed by European Standardization Organizations, with the support of concerned stakeholders. The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application."*

4.9.2 Placement of signs notifying the presence of readers

4.9.2.1 General

Notification signs should be placed at the entrance to all areas where fixed RFID readers are installed or mobile RFID readers deployed.

The sign notifies the individual that RFID readers might be operating within the signed area.

The sign does not purport to define the boundaries of the area where tags might be read, nor does it indicate the likelihood of reading of any tagged item carried by the individual.

NOTE *The energy field emitted by a reader, especially the common UHF propagating type, can vary in strength and shape over time due to changes in temperature and humidity, and also due to changes in the physical background which might absorb or reflect the signal. Even with constant reader field strengths, the range at which a tag might be read can vary considerably depending on tag antenna size, orientation, the electrical characteristics of the item to which the tag is attached, and whether the tag is fully passive, battery assisted or fully active.*

4.9.2.2 Multiple applications

Where the sign relates to multiple applications by a single operator, the purpose of these applications should be listed on a single sign. It is recommended that the description of the purpose is kept general to reduce the need to place new signs if the purpose is modified.

4.10 Presence of tags

4.10.1 General

Clause 9 of the EC recommendation [2] notes that *"On the basis of a common European sign, developed by European Standardization Organizations, with the support of concerned stakeholders, operators should inform individuals of the presence of tags that are placed on or embedded in products."*

NOTE *The "concerned stakeholders" include Government organizations, RFID application developers, RFID technology providers, Industry Associations, Standards Bodies and other operators.*

In this case, the operator is defined as the legal entity that caused the tag to be placed on, or be embedded in, the product. That entity is the only entity that can be certain that a tag has been attached to a product.

4.10.2 Use of emblem on tagged items

Notification should be performed by the application of the common RFID emblem to the tagged product. The size of the emblem may be determined by the operator, but should be legible as defined by trade regulation. The e-mark for weights and measures provides a useful comparison.

Placement of the emblem on the tagged item is at the discretion of the operator. Placement close to the tag is encouraged as good practice, especially if the tag is embedded, to improve ease of tag reading.

The colour and intensity of ink used to print the emblem is at the discretion of the operator, always subject to legibility as determined by trade regulation.

4.10.3 Purpose of application declaration on tagged items

In many cases, especially for fast-moving consumer goods, the tagged item might become part of several applications as it moves along the supply chain.

An operator might have limited or no knowledge of these additional applications. Therefore it is not practical to require a purpose of application on such items.

In the case of consumer durables, a tag embedded for warranty, maintenance and end-of-life disposal management, might be read in the premises of the individual by a mobile reader operated by a service person.

In these cases, where space permits, a sign showing the purpose of the embedded tag should be placed on the item.

For contactless cards in the financial, library and public transport sectors, the purpose of the tag should be declared to the user when the card is issued. As the card will normally only be used by the person to which it was issued, there is limited additional benefit to be gained from placing a purpose of application statement on the card itself.

4.10.4 Contact point on tagged items

In general, tagged items in the retail, library, finance and public transport sectors might already carry the legal name and contact point of the entity responsible for compliance with trade regulation.

This entity is typically also the entity that caused the product to carry a tag. Providing this is the case, existing contact point information such as customer care line may be used.

Where there is no existing contact point on the item, or the existing contact point is inappropriate for enquiries about the RFID tag, then the operator, as defined in **2.7**, should place contact information on the tagged item.

The contact point should conform to **4.5**.

4.11 Signage on tagged items

Where there is a need to tag a product, and the PIA mitigation process indicates that a notification sign becomes necessary, then it is recommended the following organizations take action whether they are operators or not:

- product manufacturers of retail goods which add RFID tags to their retail products;
- packaging suppliers which provide RFID tagged retail product packaging;
- logistics, e.g. third-party logistics providers (3PLs), which add RFID tags to retail products or retail product packaging;
- European importers which import RFID tagged retail products, or RFID tagged retail product packaging, or apply RFID tags to retail products or their retail product packaging;
- all other organizations which add RFID tags to retail products or retail product packaging.

If a retail product has a tag attached or embedded then the common European sign should be displayed on the retail product. If the product is sold inside packaging, then this packaging should also display the notification sign.

4.12 Signage on embedded tags

Embedded tags are generally used in longer life products such as consumer durables, with the intent of capturing warranty information during operation, and identifying materials at end-of-life disposal.

The length of time between manufacture and disposal, which is potentially decades, might demand that more information is held on the sign in order to avoid dependence on manufacturer held information becoming inaccessible.

Where tags are embedded in products, such as consumer durables, the full notification sign should be applied to the outside of the product where space permits.

The sign should be placed close to the embedded tag, where space permits, to ease discovery of the tag.

4.13 Guidelines on additional information

The signage system contact element should point to an information resource created and maintained by the application operator and used by the operator to answer questions from individuals about the privacy characteristics of the application. This resource should contain the operator's public information policy together with details of the application.

In general, this resource should be developed as part of the PIA process undertaken during the design and implementation of a RFID application.

The PIA process should determine the detailed information required for a particular application.

Typical information may include the following:

- What data is being collected?
- Why is the data being collected?
- How is the data being collected and stored?
- Where is the system in operation?
- When will the data be deleted?
- Who is the operator?
- Who will use the data?
- Will the data be accessible for and used by any third parties?
- A summary of the PIA.
- The likely risk to privacy.
- The risk mitigation techniques deployed.
- Residual risk.

The creation of this resource will allow the information on the sign to be minimized and generalized without reducing the effectiveness of the notification process. In turn, this will reduce the need to update the sign in the event of a new PIA process becoming necessary.

Annex A (informative) Overview of automatic identification and privacy

A.1 About automatic identification systems

This PAS focuses on implementations where data is captured using RFID systems.

However, RFID is just one of a wide range of automatic identification and data capture (AIDC) techniques upon which modern life is increasingly dependent for its efficient and safe operation. Though the methodologies differ in the techniques used, many of the underlying concepts are very similar.

It should also be appreciated that once data has been captured, the same privacy concerns exist irrespective of the data capture technique employed.

A.2 RFID systems

A.2.1 General

A RFID system typically consists of one to very many tags and one or more readers (sometimes called interrogators). The system will also contain a host to process, store and as necessary forward the data captured

A tag typically consists of an antenna to receive energy and signals to/from the interrogator, a capacitor to store a small amount of energy, and a microchip to process and respond to the interrogator's commands. On-board memory stores the data.

RFID is not a new technology, with RFID systems being used to identify planes during the early days of radar during the Second World War. Radar could be used to identify that a plane was heading in a certain direction, speed and height: the RFID transponder allowed the plane to transmit its identity "friend or foe" to the radar station, an example of combining what is it information with which is it to obtain a more complete picture.

Nor is RFID one single technology. The technologies vary in relation to:

- coupling technique between reader and chip: inductive, propagating (beam);
- method of powering the tag chip: passive, active, battery assisted passive;
- frequency used for air interface between reader and tag;
- memory size and functionality.

The performance and capability of a RFID system depends on applying the technology which is most appropriate for the planned application. It should be understood that RFID differs from a data capture system such as barcode in that it interacts with the environment in which the RFID system operates, most notably in the case of passive UHF. Changes in the environment may change the performance of the system.

RFID should not be regarded as a "silver bullet" capable of dealing with any problem. It should be viewed as one of a range of automatic identification techniques: the system selected should be chosen on the basis of its functional delivery, not on the basis of the technology itself.

A.2.2 RFID coupling techniques

A.2.2.1 General

As its name suggests, RFID is a wireless technique.

Two methods are used to provide a connection between a RFID tag and a reader (sometimes called interrogator).

A.2.2.2 Inductive

In this system, the reader and the tag are analogous to the two poles of a transformer. The reader antenna emits an inductive field which loops back on itself. The tag has a loop antenna, and if the lines of force from the reader intersect the tag antenna, then electrical energy will be induced in the tag antenna, and this can be used to energize the small microprocessor chip on board the tag.

The reader is able to resonate its antenna to encode and transmit commands to the tag, and, in the case of writable tags, data. The energized tag is also capable of transmitting digital messages back to the interrogator: this may be the data held by the tag, or in the case of the higher frequency tags, it will also support a dialogue between the tag and the reader to allow the reader to electronically singulate a tag, in order that it can read it before moving on to read another tag in the field. This singulation methodology can allow an interrogator to read several hundred tags per second.

The looping nature of an inductive energy field restricts the distance a tag can be from a reader before there is insufficient energy to drive the microprocessor in the tag. Even with systems with large antennae, emitting the maximum permitted energy, the energizing range will not exceed approx 1.25 m. Smaller and lower power systems, such as are found in most handheld readers, may have a range of a few centimetres. This range limitation can be used to good effect, especially with financial and transport RFID cards, where short range is one of several techniques which are used to protect the card from eavesdropping.

Inductive systems are largely unaffected by the presence of water in the neighbourhood of the tag. The presence of metal does have a negative effect on performance, but less so than for propagating systems.

A.2.2.3 Propagating

In this technique, the reader antenna emits a beam of radio energy which a correctly tuned antenna on a RFID tag can gather and send to the tag's microprocessor. The energized tag is then able to modulate its so-called radar reflectance profile to transmit a digital response to the interrogator. As with the inductive system this may be data or a system response to an interrogator command.

The read range of propagating systems is considerable and can be of the order of 10 m or more in ideal conditions. This brings many benefits, but introduces the risk of spurious reads of tags not in the zone of interest, leading to the need to implement mitigation to filter out these spurious reads.

NOTE *In relation to privacy and eavesdropping concerns, implementers of passive RFID systems should be aware that the limit on read range is normally the distance beyond which the interrogator can no longer reliably energize the tag's microprocessor. However, once a tag is energized by a reader, another reader may be able to read the tag at extended ranges. In the most extreme case, but still using commercial off-the-shelf equipment, an energized tag can be read at ranges of 200 m, even though the tags have to be within 8 m of an energizing beacon to stay energized.*

A.2.3 RFID powering techniques

Tags may be active (so-called because they have an on-board source of power) or passive.

NOTE *Active should not be confused with activated, which means that a tag has been powered up and is ready to respond to a reader.*

Passive tags are able to draw power from an energy field emitted by a reader/interrogator.

Some passive tags are battery assisted to help them perform well in challenging conditions where metals or liquids are in the vicinity of the tag or where the tag is distant from the reader. However, the battery is only used to power the microchip and does not boost the signal returned by the tag.

Passive tags are simpler and cheaper than active tags, but have much less performance in terms of range and ability to process information.

The various systems operate at frequencies from 125 KHz (LF) through 13.56 MHz (HF) and 850 MHz (UHF) to 960 MHz (UHF). Some active systems also operate at 433 MHz and 2.45 GHz. The higher the frequency the faster data can be transferred to and from the tag: this is important when you wish to communicate with larger numbers of tags at the same time.

The coupling of the reader and passive tag in order to transfer power and data may be inductive or propagative in nature. In an inductive system, the tag and the reader act like the two poles of a transformer: the reader is the primary coil and emits a magnetic field which intersects with the coil of the tag antenna to allow energy to be transferred to power the microchip on the tag. Once powered up, the microchip can resonate the field emitted by the tag and this detected by the reader. In a propagating system, the reader emits an electric field rather like a torch beam. The tag antenna collects energy for use by the microchip which can then modulate the ability of the tag to reflect energy back to the reader. The modulation changes can be decoded as data by the reader.

Typically, inductive systems are used at LF and HF, but inductive coupling can also be used at UHF where there is a need to read tags in the presence of liquids which would tend to absorb propagating energy but allow magnetic energy to pass through them. Also a magnetic field loops back on itself and the energy field strength decays very rapidly, allowing a short range but more precisely defined read energizing field than is possible using the longer range propagating methodology (which is normally only implemented at UHF and MW frequencies).

A note of caution is made regarding range in relation to propagating systems. Range is often the reason quoted for selecting UHF in comparison to inductive LF/HF systems, with vendors quoting ranges of 10 m and more. The reality is that read range is probabilistic in nature and the probability of a fast read tends to reduce as distance from the reader increases. Also propagating energy fields tend to have null zones due to reflected energy from walls etc. cancelling out incident energy form the interrogators.

It should also be noted that in general writing to a tag requires much more energy than reading. As a consequence, write range tends to be about half that of read range.

A.2.4 Eavesdropping of passive tags

The energy budgets for fully passive tags are highly asymmetric.

The reader needs to transmit large amounts of energy in order to energize the tag: once the tag is energized, very small amounts of energy are needed to sustain communication with the tag.

As a result, the so-called forward link from the reader to the tag is often, all things equal, the limiting factor for read range.

However, once the tag is energized, communication on the return link from the tag may be eavesdropped by other readers which simply listen and do not try to energize the tag. This "bistatic" technique can allow energized passive tags to be read for extended distances. In the case of UHF tags, this distance may be up to 200 m using specialized equipment

NOTE *Such performance might require synchronization between the energizing and reading elements of the system. Such a technique is difficult to replicate by an eavesdropping reader.*

In the case of HF tags, the effect is less marked, with ranges from 5 m to 3 m being reported.

A.2.5 Tag memory types

Last but not least, as data is the payload for these systems, various types of data storage ("memory") are used.

Read only (RO) memory is low cost and requires little energy to operate: the typically small amounts of data held in RO memory are burnt in during chip manufacture and cannot be changed.

Write once, read many times (WORM) memory allows users freedom to encode a tag with their own ID number rather than one provided by the chip manufacturer and this can significantly reduce the complexity of managing the back-office databases.

Read/write (RW) memory gives full freedom to update the memory as a tag moves along a supply chain, though this introduces risk as unauthorized parties could accidentally or deliberately write incorrect data to the chip.

Annex B (informative)
Description of the RFID application

B.1 PIA report

The RFID application operator should include, where applicable, the following 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 (e.g. frequencies)
- 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

- 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

B.2 Privacy objectives

There are currently 9 data protection objectives embedded in the Directive 95/46/EC [3].

The PIA process was developed by considering these objectives and the associated risks of RFID. This annex summarizes these data protection objectives.

While all objectives are essential elements of organizational 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 objectives is to inform the creation and development of the PIA process more than the operation of any specific PIA. Privacy objectives when outside the range of application readers will depend upon the use of the tag and the data held on the tag.

The following is a description of the data protection objectives:

Safeguarding quality of personal data

- Data avoidance and minimization, purpose specification and limitation, quality of data and transparency are the key objectives that need to be ensured.

Legitimacy of processing personal data

- Legitimacy of processing personal data should 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 should 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 should 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, correct and erase data

- It should 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 should 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 should be especially ensured.

Safeguarding confidentiality and security of processing

- Preventing unauthorized access, logging of data processing, network and transport security and preventing accidental loss of data are the key objectives that need to be ensured.

Compliance with notification requirements

- Notification about data processing, prior compliance checking and documentation are the key objectives 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 data retention or other legal requirements.

B.3 Privacy risks

A list of possible privacy risks related to the use of the RFID application under review is given in Table B.1.

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 a RFID application.

RFID application operators can use the list in Table B.1 as a starting point; however, not all of these risks might 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 might 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.

B.4 List of examples of RFID application controls and mitigating measures

B.4.1 General

This subclause provides a list of examples of potential controls that can help a RFID application operator to identify appropriate mitigating strategies.

Risks identified as relevant for a RFID application operator in stage 2 of the PIA risk process can be mitigated through one or several mitigation strategies, some of which are outlined in this annex.

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.

NOTE *These processes are additional to the existing European Union data protection regulatory framework and are not intended to replace it or modify its scope.*

B.4.2 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 minimization in handling RFID data, where feasible;
- processing or storing of information from tags that do not belong to the RFID operator;
- security governance practices.

Table B.1 – Risks that can impact on privacy objectives

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 an 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 or her 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).

Table 1 – Risks that can impact on privacy objectives *(continued)*

Privacy risk	Description and example
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, a 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 a RFID card, an ex-trainee gets access to parts of an organization 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: a 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: access to RFID employee card data is not logged.
Uncontrollable data gathering from RFID tags	The risks associated with tags both within the area of application readers and those if it should be taken beyond that operational domain for example that RFID tags could be used for regular profiling and/or tracking of individuals. Example: retailer reads all tags that they can see.

B.4.3 Providing individual access and control

Individual access and control provisions include:

- providing information about the purposes of the processing and the categories of personal data involved;
- describing of how to object to the processing of personal data or withdraw consent;
- identifying the process to request rectification or erasure of incomplete or inaccurate personal data.

B.4.4 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 recognized that back-end systems are often complex and might have been the subject of their own PIA. That analysis might 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 back-end 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.

B.4.5 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 authorization 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 or erasing the data at the end of the retention period; 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 can be at issue. Deactivation or removal are currently the two most common forms of end-user/consumer mitigation. These might 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 [2] on RFID privacy and data protection for RFID applications suggests certain methodologies and best practices associated with implementation of deactivation or removal in retail.

B.4.6 Accountability measures

Accountability measures are designed to address procedural data protection. This will raise external awareness regarding RFID applications.

One such measure might be to ensure 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) (can 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 organizational measures related to the protection of personal data and privacy;
- inquiry methods (e.g. methods through which the RFID application operator can 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.

Annex C (informative) Protecting the privacy of the individual: the EC approach to RFID

C.1 Background

The European Commission considers RFID to be a strategic element in its plans to increase the competitiveness of the EU, and deliver societal benefits to its individuals. Considerable effort is expended supporting the development of building blocks and enabling technologies for the Internet of Things (IoT). RFID is seen as a predominant source of data for the IoT.

The EC has recognized that RFID, in common with some other aspects of the IoT, lacks common governance processes in Europe, in particular a consistent approach to the protection of individuals' rights. The resulting uncertainty in implementers' minds potentially inhibits the use of RFID to meet economic and societal objectives with a further potential of backlash from consumers.

The EC commenced a structured programme of work which, among other things, will provide RFID system implementers with:

- a PIA framework consistent with the EU data protection directive; and
- a public notification signage system to make individuals aware of the presence of RFID readers.

C.2 Privacy impact assessment

C.2.1 PIA framework development process

In May 2009 the EC published the so-called EC recommendation [2], and established the RFID PIA informal working group to develop the PIA framework. This group delivered a draft to Article 29 working party in April 2010, and the PIA framework was officially endorsed on 11 February 2011 by the Article 29 working party.

NOTE 1 *Recommendation on the implementation of privacy and data protection principles in applications supported by RFID.*

NOTE 2 *The Article 29 working party refers to a consultative body composed of representatives of national data protection authorities at the EU level.*

The PIA framework document provides a high-level application-agnostic tool to allow RFID system implementers to assess and document RFID applications in a consistent way regarding their compliance with EC privacy and data protection protocols.

An agreement on implementing the framework was reached between the EC and industry representatives.

This was subsequently signed on 6 April 2011 by Neelie Kroes, Vice President of the European Commission in charge of the digital agenda, as well as Mr. Kohnstamm (Chair of Article 29 WP), Pr. Helmbrecht (Executive Director of the European Network and Information Security Agency [ENISA]) and industry representatives (GS1, ERRT, AIM Germany, Bitkom, Deutsche Post/DHL, and Eurocommerce).

Neelie Kroes noted that the "agreement puts consumers' privacy at the centre of (RFID) technology and (makes) sure privacy concerns are addressed before products are placed on the market" and that the agreement was a good example of how industry should work with consumers, privacy watchdogs and others to address legitimate concerns over data privacy and security related to the use of RFID tags.

The EC sees this agreement as highly significant: the co-regulation of the EC and industry contained in the agreement is seen as a model for the future of ICT standardization. The phase 2 of mandate 436 [1] will contain more detailed RFID PIA process and methodologies applicable to the framework.

C.2.2 Common RFID notification sign

A common RFID notification signage system was developed by CEN as a technical specification, PR/CEN/TS 00225069-2012.

This specification comprises three elements, a common emblem for recognition purposes, the scope of the RFID system being notified, and the contact point from where more information about the RFID system can be obtained.

Annex D (informative)
Case studies for the use of RFID notification signage

D.1 General

The following illustrations developed by RFID in Europe and contained in the EC Draft Guidelines for RFID notification sign [4] do not explore all combinations of possible choices but rather offer a selected consideration of likely scenarios based upon dialogue with stakeholders.

D.2 Shoe manufacturer

A manufacturer of shoes destined for European retailers wishes to attach RFID tag embedded labels to their shoes. The manufacturer's processes verify the RFID tag by performing a read operation with a RFID reader application or equivalent. The manufacturer records the RFID tag identifier and/or encodes an identifier in the RFID tag memory. The manufacturer as the RFID operator ensures that the common European sign appears:

- on the RFID tag label attached to the shoe;
- on the external surface of all packaging the manufacturer supplies which might be presented to the retail consumer.

The manufacturer may display the common European sign elsewhere. Suggestions include:

- on their website in association with any pages introducing the RFID tagged product to the public or, describing the manufacturer's use of RFID or, similar ways which support a RFID information campaign;
- on media accompanying the product which references RFID, e.g. a user instruction guide which mentions RFID, a ticket which indicates how to remove a RFID tag, a cleaning instruction label which mentions how to preserve the RFID tag for consumer use, etc.;
- where the manufacturer offers the RFID tag labelled shoes directly to consumers through catalogues, or Internet sales, or any other direct to consumer channel then the manufacturer ensures that the common European sign appears on all media offering the RFID tag labelled shoes for sale to the public. This allows the potential consumer to be notified and informed prior to purchasing or receiving the goods.

D.3 Retailer

A retailer wishes to install RFID readers in order to monitor and confirm goods receipt in their back-store areas. The retailer operates the RFID application and ensures that the common European sign is displayed at all location entrances to the areas where there are one or more RFID readers installed.

As a stakeholder, the retailer assists the operators and other stakeholders to ensure suitable consumer and public notification of the presence of RFID-tag-embedded or attached retail items.

D.4 Public transport provider

A public transport provider wishes to offer RFID based contactless payment or consumer identification cards associated with payment. The public transport provider contracts the operation of the application to a third party.

The third party is a RFID operator as they are responsible for the RFID application. The third party operating the RFID application ensures that:

- all entrances to the public transport provider locations where there are RFID readers, display the common European sign;
- all locations where the public interact with RFID readers display the common European sign;
- the RFID based contactless payment or consumer identification cards are purchased by consumers and are therefore retailed items.

The supplier of the RFID based contactless payment or consumer identification cards ensure that:

- each card displays the common European sign; and
- all card packaging which might be presented to the consumer displays the common European sign.

D.5 Public service organization

An administration organization seeks to have, or has, RFID-based contactless building entrance, lift, access doors to each floor and meeting room access control application. Each employee and guest is registered and issued with RFID badges which are read by fixed installation RFID readers located at entrances to the building, lift, access doors to each floor and meeting rooms.

The administration organization leases the building and a third party security provider operates the access control system. The third party security provider is the operator of the RFID application and ensures that:

- at each building entrance the common European sign is displayed;
- at each RFID reader location the common European sign is displayed;
- each RFID tag badge is labelled with the common European sign.

NOTE *The third party security provider may legitimately seek the cooperation or participation of the building owner and/or, the owner of the access control system in fulfilling the above.*

Bibliography

Standards publications

BS ISO/IEC 29160, *Information technology – Radio frequency identification for item management. RFID Emblem*

PR/CEN/TS 00225069-2012**,** *Information technology – Notification of RFID – The information sign and additional information to be provided by operators of RFID application systems*

Other publications

[1] European Communities. Mandate 436 on Information and communication technologies applied to radio frequency identification (RFID) systems;

[2] European Communities. EC Recommendation COM (2009) 3200 final on the implementation of privacy and data protection principles in applications supported by RFID; 12 May 2009

[3] European Communities. EC Directive 95/46/EC on the protection of individuals with regard the processing of personal data and on the free movement of such data; 24 October 1995

[4] European Communities. Guidelines on the Use of the Common European RFID sign; 28 July 2011, Draft Version 1 EC INFSO

Further reading

A Digital Agenda for Europe EC COM (2010)245 final/2

A strategic vision for European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020 EC COM (2011)311 final

European Communities*. 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; 12 May 2009, SEC (2009) 586

European Communities. EC Directive 2009/136/EC amending Directive 2002/22/EC on universal service and user's rights relating to electronic communication networks and services.

European RFID Guide sets NFC Privacy Guidelines; Eric Doyle; eWeek Europe April 2011

Guidelines on the Use of the Common European RFID sign; 28 July 2011, Draft Version 1 EC INFSO

Privacy Code of Conduct for RFID Technologies; Toby Stevens; RFID Today, October 2007

Proposal for a Regulation of the European Parliament and European Council on European Standardization EC COM (2011)315 final

The RFID Privacy and Data Protection Impact Assessment Framework in the EU: The Article 29 Working Party and the FTC are in no rush; February 19th, 2011: Monique Altheim

Websites

Guidelines on the Use of the Common European RFID Sign

http://economie.fgov.be/fr/binaries/Guidelines%20for%20use%20of%20the%20Common%20European%20RFID%20Sign_tcm326-165637.pdf

Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011

http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

Privacy Impact Assessment Handbook:

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:

http://ec.europa.eu/justice/data-protection/law/status-implementation/index_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:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)845 086 9001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)845 086 9001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)845 086 9001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)845 086 9001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **http://shop.bsigroup.com/bsol**

Further information about British Standards is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-580-76452-3