ENISA Position on the

Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications [of March 31, 2010]

July 2010

ABOUT ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors.

http://www.enisa.europa.eu/

A. Background Information

On the 12th of May 2009, the European Commission published a recommendation "on the implementation of privacy and data protection principles in applications supported by radio-frequency identification"[1], which considers that the "member states should ensure that the industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments (PIA)".

Based on this, the European Commission set up an informal "Working group on the implementation of RFID communication"[2] to work on the development of a PIA Framework. On March 31st 2010, industry representatives delivered a draft Privacy and Data Protection Impact Assessment Framework proposal, which has been published in the European Commission's RFID web-page and has also been sent to Working Party 29 for endorsement.

According to Recital 17 of the RFID Recommendation, the development of the PIA Framework "should build on existing practices and experiences gained in Member States, in third countries and in the work conducted by the European Network and Information Security Agency (ENISA)". Also ENISA has expertise and experience in risk assessment methodologies, in building a risk assessment framework on identifying emerging and future risks[3], and in particular in deploying this framework to identify emerging and future risks of a prospective Internet of Things / RFID environment in a recently published study[4]. Given the above, we have been asked by the European Commission to provide our comments and recommendations on the draft of the PIA framework.

B. Introduction

Benefits of the PIA process

ENISA considers the development of an appropriate PIA process for RFID applications as necessary and an appropriate solution towards addressing privacy challenges. Specifically, ENISA believes that the benefits of the PIA process are the following:

- Proactively identify major impacts and risks of the RFID application with regard to privacy: this will increase efficiency in the development of the application, since it will already have some necessary built-in features
- Enhance product marketability and reputation of the organisations developing the application
- Minimising challenges in complying with data protection legislation
- Minimise costs that would occur from having to apply controls and countermeasures after deployment of the application

[1] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[2] http://ec.europa.eu/information_society/policy/rfid/documents/participateinworkgroup.pdf
[3] More information on the ENISA EFR Framework is available at: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual
[4] "*Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology*", available at: http://www.enisa.europa.eu/media/press-releases/flying-2.0-study-of-internet-of-things-rfid-in-air-travel

- Enhance citizens' trust in applications

Objectives of the PIA process

Based on this, ENISA considers that the objectives of the PIA framework are:

- To promote and to ensure a proactive approach in identifying and addressing risks related to privacy & data protection in RFID applications, in the context of the "privacy by design" and precautionary principle
- To provide a generic and comprehensive PIA approach that the industry can deploy, and which can be ideally integrated with the other business procedures of the organisation, so as to facilitate its deployment
- To ensure that the approach generates the appropriate information to be provided to the competent authority
- To provide a flexible approach that enables appropriate identification of risks for complex systems and applications, while it is not cumbersome or detailed when there is no need to do so

About this document

ENISA supports the initiative to develop a PIA framework to be deployed by RFID Application Owners. We believe that such a framework would enhance and further promote solutions of "privacy-by-design".

Our comments have been based on the official draft of the industry proposal published in the European Commission web-site[5] and submitted to Article 29 Working Party.

In our comments, we identify certain issues and areas for improvement of the current PIA draft. Given our experience and expertise, our comments are mostly related to the methodological part used (particularly regarding risk management and impact assessment) and not on legal issues. Most of the comments presented here are high level comments. Based on these comments we make some recommendations, which we think could substantially improve the current PIA draft. Notably, we have considered two viewpoints when making the comments: of the **competent authority**, who will receive the PIA reports, considering what information they need to receive, and of the **RFID application owners**, who would be performing the PIA process, considering making the process as clear and as efficient as possible.

[5] http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf

C. Comments on the PIA draft

First of all, we are pleased to say that ENISA finds in this draft a very good starting point towards establishing a PIA framework. In principle, as also see from the previous section, we concur with the objectives and purpose of the PIA framework presented therein.

Based on the objectives of the PIA presented in the previous paragraph, ENISA has identified some major issues and areas of improvement in the proposed PIA framework.

1. LACK OF OR INAPPROPRIATE METHODOLOGICAL APPROACH USED IN THE PIA DRAFT

The PIA framework draft is not based or does not follow a tested and comprehensive risk methodological basis, e.g. a risk management and an impact assessment methodology. This is our major finding, which we find that it generates a lot of subsequent issues with the PIA draft, which are explained below. Not having a structured approach in place, the identified steps of the PIA process are not always clear, they overlap. Please see comments below for additional issues that this creates.

It is also noted that it is not clear in the PIA draft if it has taken stock of existing PIA initiatives in other countries (e.g. UK, USA, Canada, Australia, and New Zealand) and similar practices already used in some industry organisations.

2. STRUCTURE AND COHERENCE ISSUES

As mentioned above, in certain places the PIA process ceases to be coherent and the objectives of all steps of the PIA process are not always clear, or they change, the order of various steps is confusing and overlapping of steps seems to be taking place. For example:

- A classification exercise on RFID applications precedes any analysis; it is not clear what is the value of an analysis when it is limited at the end of the process ("Part D – Analysis and Resolution")
- The identification of RFID application scope takes place before the initial assessment / classification of RFID applications.
- In section 2.3, in the first bullet point, it is mentioned that particular attention should be paid to "*whether the information in RFID tags contains personal data as defined in Directive 95/46/EC*", where in fact this has already been covered in 2.1 (and 1.5, but it is not clear if this is a step or not). Also in 2.3.7 the section "*RFID Application Classification*" refers to section 1.5, which confuses as to the order of the steps that need to be followed, since the reader is asked to go back and forth.
- In Chapter 2, the "Initial analysis" step is almost the same with the section 1.5 titled "Classification criteria of RFID Applications", apart from one question that is mentioned in 2.1 but is not considered in 1.5. It is not clear what the distinction is or if these are two different steps etc.

3. INAPPROPRIATE SIMPLIFICATION OR COMPLEXITY OF CRITICAL STEPS

We have noticed that certain steps are oversimplified, while at the same time they might involve some increased level of complexity which is not appropriate. In particular:

a. Classification of RFID applications:

- The criteria they consider only the containing of personal data within an RFID tag, where according to the definition of the RFID application in the RFID communication this includes, the RFID tag, RFID reader, the back-end application and any telecommunication infrastructure
- The criteria used are simplistic: apart from the first bullet point, the "classification" in a risk management approach or a business impact assessment approach is the result of proper impact assessment and analysis
- It seems that this classification is performed in order to arrive to a decision on whether to perform the PIA or not. Since the decision is binary, there is no apparent reason to classify RFID applications in four different levels ***at this stage of the assessment***. This increases the level of complexity at this stage of the assessment, without providing clear added value.

b. Final section on decision on RFID deployment or not

The binary option here is not appropriate and might lead to inappropriate decisions. Since this is an umbrella and generic framework, it would need to cover most of cases, and identify also "grey" areas: it might well be the case that the result of the privacy impact assessment and analysis cannot be one or the other, e.g. that the application might be deployable, should certain conditions be met (i.e. controls to be included in the system).

4. RFID APPLICATION OWNERS ARE NOT CLEARLY ASKED TO IDENTIFY RISKS AND IMPACTS

While we have already identified a lack of a comprehensive methodological basis of the PIA process itself, the PIA process proposed does not provide clear guidelines to the RFID application owners to identify the major risks and impacts regarding privacy & data protection that could be generated by the RFID application under review. The process presented in paragraph 2.4 under the "PIA report" section, which basically lists the contents of a PIA report (see comment 5 below), it clearly considers controls identified by the RFID application owners, but not the impacts and risks potentially generated by the application. It is not possible however to identify appropriate controls if even a basic risk assessment has not been performed yet, as one wouldn't know what to protect and from what (e.g. vulnerability, threat). So it looks as if there is a step missing from the process presented.

5. THE FOCUS SEEMS TO BE ON REPORTING RATHER THAN ON THE PROCESS ITSELF

In the second chapter ("*The PIA Process*"), the second section after the initial analysis is on the PIA report Structure and Content. We think this is an issue stemming from the lack of following a particular methodology in developing the PIA approach. Making the report should not be confused with the whole PIA process: the emphasis should be on the latter, given the objectives of the PIA framework (see specific recommendations in the section below).

6. TIME TO PERFORM PIA IN THE DEVELOPMENT LIFE-CYCLE OF THE APPLICATIONS IS NOT CLEAR

It is indicated in the PIA draft that the PIA should be performed "before the deployment" of the application, while in another place it is described as "at the early stages of the specification or development process". It does not specify at which specific stage of the development life-cycle of the applications, something which may generate confusion when the RFID application owners deploy the PIA process, as to when to perform the PIA.

7. NOT CONSISTENT / NO PROPER USE OF TERMINOLOGY

We have noted that throughout the document some terms are used interchangeably or without proper definition. Specifically:

- Terms like 'PIA framework', 'PIA process', 'PIA approach' are used interchangeably, despite of the initial definition distinguishing 'PIA framework' from 'PIA process'
- The terms 'impact' vs. 'implications', 'initial analysis', 'classification', 'redress methods', 'supporting artefacts, 'governing practices'
- In the criteria for classification of the RFID applications, in section 1.5, the terms 'collect', 'contain', 'process', 'transfer' of personal data; in fact these may be considered different actions with different impacts

8. IMPLEMENTED SYSTEMS VERSUS SYSTEMS UNDER DEVELOPMENT

The approach in the draft interchanges between assessment of *existing / implemented systems applications* and *impact assessment of applications / systems to be developed*, so as to ensure privacy-by-design. This is very important to clarify, especially in terms of scope of the PIA. You cannot follow the same approach in both cases, since it cannot be effective.

9. WORKFLOW DIAGRAMS IN APPENDIX C ARE NOT CLEAR

It is a very good idea to have a schematic representation of the steps of the PIA process. However the diagrams provided in the Appendix of the PIA draft are not clear enough: the workflow and the steps to be followed are somewhat confusing to follow, in terms of workflow steps to follow, critical decision steps etc.

D. Recommendations

Based on the issues identified and presented above and also in view of the objectives of this document, we have identified some recommendation in order to improve the current document. The recommendations are not all one to one with the comments identified in the previous section, since one recommendation may be deemed to address more than one comments.

1. IDENTIFY AND ADOPT A COMPREHENSIVE AND RECOGNISED METHODOLOGICAL BASIS TO IMPROVE THE PIA FRAMEWORK: *CONSIDER EXISTING FRAMEWORKS, STANDARDS AND PRACTICES*

Considering the purposes of the Privacy Impact Assessment (identification of risks and the impact, identification of appropriate controls to mitigate the risks in a proactive way) and the fact that this kind of procedure is relatively new, its development should be based on existing methodologies, especially on risk management.

As quoted in the RFID communication document "*The use of international standards, such as those developed by the International Organisation for Standardisation (ISO), codes of conduct and best practices which are compliant with the EU regulatory framework can help to manage information security and privacy measures throughout the whole RFID-enabled business process*". Indeed, an example of such a risk management framework that can be considered is the ISO/IEC 27005[6]. Considering such an established methodology, will assist in shaping up the approach, address many of the issues identified in the previous section, and add to the credibility of the PIA Framework.

Notably, in the development of this framework, other similar country and corporate initiatives should be taken into account at an international level, e.g. UK, USA, Canada, Australia, and New Zealand. There is also an ISO Standard (ISO 22307:2008) on Privacy Impact Assessment in Financial Services, which although has a different focus (financial services), it might provide a helpful input in developing the PIA draft for the purposes of RFID applications. While we do not recommend adopting these existing processes and frameworks as they are, we believe they should be considered, since they can offer valuable guidelines and ideas that the drafted PIA process can benefit from.

2. IDENTIFICATION OF RISKS AND IMPACTS SHOULD BE CLEARLY REQUIRED OF THE RFID APPLICATION OWNERS

At this point, we should highlight that apart from the risk management methodology we are proposing above to be considered in the development if the PIA process, the PIA framework itself should require the RFID application owners to perform an appropriate risk management exercise. Specifically and while it should not oblige the owners to use a specific risk management methodology, it should however identify the major steps that the RFID application owners need to perform. We understand that the PIA framework itself is not and should not be a risk assessment of prospective RFID applications; it should however clearly request the RFID application owners to perform risk management.

[6] International Standard ISO/ IEC 27005:2008 Information technology — Security techniques —Information Security Risk Management, 2008

We recommend that the analysis part of the PIA process includes and requests from the RFID application owners to perform at least the following[7]:

- **Identifying the system of reference**: the scope and objectives of the RFID applications, the stakeholders involved and their role, all the assets involved in the application
- **Setting the criteria against which the impact on privacy is determined**, especially if different from the ones identified in the PIA document [see recommendation 6 below]
- **Identify and evaluate the risks**: this would mean, identifying the vulnerabilities and threats, and estimating a risk value
- **Identifying the acceptance risk levels**: levels that determine whether the risks can be accepted or not; this means that some risks might be considered as acceptable.
- **Identifying appropriate mitigation strategies**: identification of controls and countermeasures to address the risks that are not accepted

The PIA's output would be a report containing at least the above items, so as to provide the Competent Authority with the appropriate information. It is important to highlight also based on our comments above, that the controls should be identified only after the privacy impacts and risks posed by the RFID application are appropriately identified and assessed, so as to allow for efficient and effective protection.

The PIA framework can also develop and provide templates[8] to assist the RFID application owners to implement it.

3. IMPROVE PIA PROCESS STRUCTURE AND ADDRESS COHERENCE ISSUES

This recommendation is closely connected to the two recommendation made above, since by following these, the PIA process structure can be significantly improved. In addition, as identified in comment 4, in the current PIA draft the PIA process, apart from the initial assessment section, includes mainly a reporting view. This entails the risk that the analysis may not be that clear to the owners, and they perform it poorly. Reporting is normally the final stage of a process and framework, containing the results of the analysis. A clear distinction between these various phases of the process should be thus made.

Regarding the reporting phase, which is by all means very important since it should deliver the appropriate information to the competent authority, PIA report template(s) should be ideally provided in the document. This will assist the RFID application owners in preparing their PIA reports; saving time and ensuring that the report will contain all the appropriate information to be submitted to the competent authority.

Regarding the oversimplification of critical steps (see comment 3), we recommend the following:

- The classification of RFID applications cannot take place at the beginning of the PIA process, nor should it be mentioned in two different parts of the process for clarity purposes. Basically, what

[7] It is noted that this is an indicative list and it by no means constitutes a detailed or an exhaustive analysis of the steps to be performed.

[8] As an indicative example of such an initiative, please refer to the "Technical Guidelines RFID as Templates for the PIA Framework" recently developed by the BSI: https://www.bsi.bund.de/cln_165/ContentBSI/Publikationen/TechnischeRichtlinien/tr03126/index_htm.html

is sought at the initial stage of a PIA is **a decision on whether to perform a PIA process at all or not** and not to classify the RFID applications. Given our comments above (and especially comments 2, 3a and 7), the existing criteria mentioned in the PIA draft to make this decision should be appropriately revisited and improved. See also recommendation 6 below.

- If a classification scheme approach is decided upon, then this should certainly provide a clear description of what the various levels mean and it should be decided at least after an initial analysis. This may also provide a basis on which different steps are used according to the required detail and granularity levels of the assessment, e.g. if a 'light' PIA is required or a more detailed one.
- Regarding the final stage, the resolution:

  (a) It should not seek a simple 'yes' or 'no' decision. The analysis would usually result in a list of potential risks, ways to address them and any remaining risks that have been accepted (i.e. no controls will be implemented to mitigate those risks).

  (b) The PIA draft should clearly indicate the role of each stakeholder in this, i.e. the RFID application owner and the competent authority. At a minimum, in the PIA report and the resolution, the RFID application owner should clearly indicate the risks, their impact, the controls identified and any risks they have chosen to accept.

  ENISA also recommends that a discussion and mutual agreement between the industry and the competent authorities as to the level and kind of information they would require at the resolution part of the PIA report may help in improving this.

Once the changes on the structure of the document has been decided upon (if ENISA's recommendation to revisit the structure is followed), a schematic representation of the final PIA process is certainly advisable. Based on comment 9 above, we would recommend updating the diagrams appropriately with the changes made, to properly reflect the workflow of the PIA process, its staring point, the various steps, the decision points etc. We believe this will provide a clear overview to the RFID application owners on how to perform the PIA.

4. CLEARLY INDICATE THE 'TIMING' OF WHEN THE PIA IS TO BE PERFORMED BY RFID APPLICATION OWNERS

As indicated in comment 3 above, the specific stage of the development life-cycle of the RFID applications during which the PIA should be performed, is not clearly indicated in the PIA document. The phrase 'before deployment' used in the document is quite vague and may in fact mean many stages in the application development life cycle. It is crucial to perform the PIA at the right time, when the owner has enough information to perform it, while they have not started implementing major parts of the system yet. Performing the PIA too late in the development process would result in time inefficiencies and additional costs occurred if the application owner finds that some parts of the application would need to be changed; while, performing it too early, when not enough information is known about the application, would yield results of no or limited value. It is thus recommended to make this clear in the PIA document.

5. DISTINCT APPROACH IN CASE OF *EX-ANTE* OR *EX-POST* PERFORMANCE OF THE PIA PROCESS

We understand that some RFID applications might be already in place or being finalising or in the last development stages, when their owners would be requested to perform the PIAs. In these cases, the approach regarding PIA should be different than that used for applications that are now under

development. Although the major steps and reporting requirements might be largely the same, some steps are bound to differ, as well as controls identified to address the risks. The PIA process should appropriately reflect this, identifying these steps, so as to provide a proper approach to be used in both cases. Considering an appropriate methodological basis when developing the PIA would assist in addressing this need.

If such a distinction is not appropriate or falls out of the purposes of this PIA framework, it should be then clearly identified so in the document, e.g. that the PIA framework regards only *ex-ante* PIAs.

6. PROPERLY IDENTIFY THE BASIC CRITERIA / REQUIREMENTS THAT DETERMINE THE PRIVACY EXPOSURE

Even if an appropriate methodological basis is identified and used in developing the PIA process, and also whichever methodology is used, there are some elements that would need to be determined within the PIA process, which the methodologies do not (and cannot) define in an absolute way. Since a privacy impact assessment needs to be performed, the criteria and requirements determining the privacy exposure would need to be properly identified. In the current document, some criteria used are whether the RFID tag contains private data, sensitive data etc; we have already considered these as simplistic (see comment 3), especially since there are more factors that need to be considered in order to determine this. It may be beneficial to determine such criteria through interaction between industry and other stakeholders, especially Article 29.