ARTICLE 29 DATA PROTECTION WORKING PARTY

00066/10/EN
WP 175

Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

Adopted on 13 July 2010

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Table of Contents

1 Context

1.1 Introduction

On May 12th, the European Commission issued a recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification[1].

Point 4 of this recommendation states that "*Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union" (emphasis added).*

According to the recommendation, once this framework for privacy and data protection impact assessments is defined, Member States should ensure that RFID operators conduct a privacy and data protection impact assessment (PIA) of RFID applications before they are deployed. Member States should also ensure that the RFID operators will make the resulting PIA Reports available to the competent authority (i.e. the DPA).

In July 2009, an informal "RFID workgroup" led by industry representatives began working on the definition of a PIA Framework, while holding regular meetings with stakeholders including consumer groups, standardization bodies, and university scholars. On March 31st 2010, industry representatives delivered a Privacy and data protection Impact Assessment Framework proposal to Working Party 29 for endorsement. **This opinion formalizes the response of the Working Party to this proposal.**

In the following, the "RFID Recommendation" shall refer to the European Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, published on May 12th, 2009. The "Proposed Framework" or simply "Framework" shall refer to the RFID Application Privacy and Data Protection Impact Assessment Framework, transmitted to Working Party 29 on March 31st, 2010 and reproduced in the Appendix of this opinion.

1.2 RFID and data protection

In January 2005, the Working Party adopted a *working document*[2] *on data protection issues related to RFID technology* (WP 105), which recognized the obvious advantages offered by RFID technology but also highlighted potential concerns on the data protection front, which arise in particular from "*the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals"*. This document noted that "*the ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories*

[1] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf

worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns."

This working document was then put up for public consultation. The result of this process was summarized in a document (WP 111)[3] published by the Working Party in September 2005. The results showed that while "*most universities, think tanks, individuals and companies providing security solutions suggested the need for some sort of additional guidance from Working Party 29*," and some suggested "*complementing the data protection Directive with specific rules for RFID"*, the industry pleaded for a "*self regulatory approach"*.

In this global context, and in coordination with stakeholders including representatives of the RFID industry, data protection and consumer rights organizations, the European Commission took the lead in developing a recommendation[4] "*on the implementation of privacy and data protection principles in applications supported by radio-frequency identification"*, which is designed to provide "*guidance to Member States on the design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data*."

This recommendation, published in May 2009, contains a strong novelty: it requires RFID Operator to conduct a "Privacy and Data Protection Impact Assessment" before an RFID Application is deployed, and make its results available to the competent authority. This new approach, acting as a complement to the existing regulatory framework provided in the Data Protection Directive and the ePrivacy Directive, provides an opportunity for the industry to demonstrate the potential of self regulation as complementary, flexible and efficient tool to the EU legal framework in the face of a rapid changing technological landscape. The Working Party supports[5] "*carrying out privacy impact assessments, particularly for certain data processing operations deemed to present specific risks to the rights and freedoms of data subjects"*. It also believes that the success or the failure of this approach is likely to either pave the way for the use of PIAs in other domains or to trigger a stronger regulatory approach.

The RFID Recommendation is also designed to promote "*information and transparency on RFID use"*, in particular through the development of *"a common European sign developed by European Standardisation Organisations, with the support of concerned stakeholders"*, designed "*to inform individuals of the presence of readers"*. Such initiative has the full support of the Working Party.

Though the RFID Recommendation explicitly refers to the Directive 95/46/EC, in some occasions, it departs from terminology traditionally used in data protection legislation, in particular when referring to "persons", "individuals" or "users". To avoid ambiguity, this opinion will use the word "person" to refer to a natural person as in Article 2 of Directive 95/46/EC, while words "User" and "Individual", with their first letter capitalized will conserve the meaning they have in the RFID Recommendation. In particular, the word "person" can be used to refer broadly both to "Users" and "Individuals", which are otherwise distinct categories of persons according to the definitions set forth in Point 3 the RFID Recommendation, which are repeated in the proposed framework. For consistency with the RFID Recommendation, this

---

3 "*Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology"*, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf

4 http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

5 See "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", WP 168, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf

opinion will also refer to "RFID Operators" instead of "data controllers", though these terms are not strictly equivalent.

In November 2009, European legislators amended the ePrivacy Directive[6] and explicitly referenced RFID technology. In recital 56 of Dir. 2009/136/EC, they recognized that "*the wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens"*, but also that "*to achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded"*. Furthermore, they added that "*when such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply"*. As a consequence, the scope of the ePrivacy directive (defined in Article 3) was revised to include "*public communications networks supporting data collection and identification devices*."

1.3 Objectives of the PIA framework

With the RFID Recommendation, the European Commission created a PIA process that aims to achieve several benefits:

- First, a PIA should favour "Privacy by Design" by helping data controllers to address privacy and data protection before a product or service is deployed. This not only benefits individuals but also data controllers by avoiding the significant costs (and often unsatisfactory solutions) that often arise when privacy features must be "bolted on" to an already deployed product.

- Second, a PIA should help data controllers to address privacy and data protection risks in a comprehensive manner. Indeed, the PIA is part of the tools that can help to assess privacy risks and find technical and organizational measures to protect personal data against unauthorized disclosure or access and to cover other security obligations established in article 17 of the Data Protection Directive and article 4 of the amended 2002/58 Directive. This process also provides an opportunity to reduce legal uncertainty and avoid the loss of trust from the public that could otherwise burden the data controller when data protection issues are not addressed appropriately.

- Finally, PIAs may help both data controllers and data protection authorities to gain more insight into the privacy and data protection aspects of RFID Applications. Performing a PIA should help data controllers to understand and implement the principles that are set forth in Directive 95/46/EC, the newly amended Directive 2002/58/EC, and in the RFID Recommendation. Information from PIAs may help DPAs identify best practices regarding the way data protection

[6] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

is implemented by the industry and, in those member states that require prior checking of (some or all) RFID applications, it may simplify the process for both DPAs and data controllers[7].

Additionally, the Working Party sees the development of PIAs as a contributing factor to the competiveness of the European RFID industry by fostering innovative approaches to address data protection and privacy issues, through technologies such as data anonymisation, partial tag deactivation, lightweight cryptography, etc.

While the PIA Framework envisioned in the Recommendation is intended to promote "Security and privacy by design" by targeting RFID Applications before their deployment, there are already many existing deployed RFID Applications. The Working Party hopes that stakeholders will capitalize on this experience and seize this opportunity to create assessment tools that can be applied to existing RFID Applications.

1.4 Summary of the proposed Framework

The proposed framework first classifies an RFID Application into 4 possible levels. "Level 0" applications, which essentially cover RFID applications that do not process personal data and where tags are only manipulated by Users, are excluded from conducting a PIA. While the term "User" can potentially cover employees, the definition of Level 0 cannot be understood to encompass an application that would be designed to monitor employees, since such monitoring would require the storage of personal data somewhere in the application. Consequently, the Working Party agrees that excluding "Level 0 applications" from the PIA process is unlikely to cause prejudice to data protection and privacy goals.

Level 1 applications cover applications where no personal data is processed, yet the tags are carried by Individuals. Level 2 applications are applications that process personal data, but where the tags themselves do not contain personal data. Finally, level 3 applications are applications where the tags contain personal data. As highlighted below in section 2.4, the use of the terms "personal data" is somewhat ambiguous in the Proposed Framework when it refers to information contained in the tag.

If the RFID Application level is determined to be 1 or above, the RFID Operator is then required to conduct a four part analysis of the application, with a level of detail that is proportionate to identified privacy and data protection implications. The first part is used to describe the RFID Application. The second part allows highlighting control and security measures. The third part addresses user information and rights. The final part of the proposed PIA framework requires the RFID Operator to conclude whether or not the RFID Application is ready for deployment. As a result of the PIA process, the RFID Operator will produce a PIA Report that will be made available to the competent authority.

[7] In this context, point 5 d. of the RFID Recommendation provides that operators, notwithstanding their other obligations pursuant to Directive 95/46/EC, should make the assessment available to the competent authority at least six weeks before the deployment of the application. The manner in which the PIA should be made available (e.g. on request or not) will be determined by the national DPAs. In particular, the risks related to the application may be taken into account, as well as other factors such as the presence of a data protection official.

The authors of the proposed Framework envision that, for some sector specific needs, the industry may translate the Framework into specific "PIA Templates" to facilitate implementation. The "PIA Report" will then be built from the sector specific template instead of the more general Framework.

2 Analysis

The Working Party acknowledges the broad work conducted by the authors of the proposed framework, and subscribes to its main goals, highlighted in its introductory sections.

While the global outline of the proposed framework does not raise particular questions, the Working Party has identified 3 critical concerns in its content, as well as some remarks, which are detailed hereafter.

2.1 Risk assessment

The introductory section of the proposed Framework unambiguously states that "*the PIA process is designed to uncover the privacy risks associated with an RFID Application* […] *and evaluate the steps taken to address those risks*." **However, this central tenet of a PIA process is absent in the content of the proposed Framework**.

Indeed, whereas the proposed Framework contains scattered references to risk assessment (mainly in its introductory parts) no section explicitly requires the RFID Operator to indentify or "*uncover privacy risks associated with an RFID Application"*. It follows that it is not possible to "*evaluate the steps taken to address those risks"*. Instead, the proposed framework only requires the RFID Operator to list the various protections and controls that have been put in place to protect privacy and personal data in the RFID application. This cannot be considered as a satisfactory means to give the RFID Operator or the competent authority a reasonable assurance that the proposed measures are adequate or proportionate to the risks, since these risks have not been identified in the first place.

The Working Party deeply regrets that this point has not been addressed by the authors of the proposed Framework.

A privacy and data protection impact assessment framework should, by definition, propose a general methodology containing a risk assessment phase as a key component. The RFID Industry certainly already implements risk assessments as part of a methodological approach in the context of information security management, such as defined in ISO/IEC 27005[8] and other national or international standards. The Working Party is convinced that the RFID Industry could build upon this body of expertise in traditional information security management to enrich the Proposed Framework with a relevant risk assessment approach. This would also impact other specific elements in the proposed Framework as notably highlighted in sections 2.2, 2.3 and 2.4 of this opinion.

[8] See ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

Additionally, Recital 17 of the RFID Recommendation considers that 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)"*. This provides a legitimate mandate for the authors of the proposed Framework to take a careful consideration at the opinion recently adopted by the ENISA on the PIA Framework[9] and request further guidance from the EU agency on the implementation of a risk assessment approach in the context of RFID. ENISA has specifically undertaken[10] "*the task to identify and assess emerging and future risks of a particular IoT/RFID scenario*, notably *in the context of ENISA's role in this specified in EC Communication "Internet of Things – An Action Plan for Europe[11]""*. **The Working Party strongly encourages the industry to seize this opportunity**.

2.2 Tags carried by persons

One of the 3 main privacy concerns highlighted in the *Working document on data protection issues related to RFID technology* (WP 105)[12] "*arises from uses of RFID technology which entail individual tracking and obtaining access to personal data"*. Indeed, tagged items carried by a person contain unique identifiers that could be read remotely. In turn, these unique identifiers could be used to recognize that particular person through time, thus making him "identifiable". This may be desirable in some cases, in particular if a tagged item is specifically designed to be used as an access control mechanism (ex: a badge). But in other cases, it raises the possibility that a person will be tracked[13] without his knowledge by a third party. As highlighted in *Opinion 4/2007 on the concept of personal data* (WP 136)[14], when a unique identifier is associated to a person, it falls in the definition of personal data set forth in Directive 95/46/EC, regardless of the fact that the "social identity" (name, address, etc.) of the person remains unknown (i.e. he is "identifiable" but not necessarily "identified").

Additionally, the unique number contained in a tag can also serve as a means to remotely identify the nature of items carried by a person, which in turn may reveal information about social status, health, or more. Thus, even in those cases where a tag contains solely a number that is unique within a particular context, and no additional personal data, care must be taken to address potential privacy and security issues if the tag is going to be carried by persons.

The Working Party welcomes the fact that the industry has recognized this issue in the PIA Framework by requiring a PIA when "*item level tags are intended to be possessed by individuals*" ("level 1" applications).

---

9 ENISA Opinion on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, July 2010, http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

10 See for example the ENISA report entitled "Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology".

11 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Internet of Things — An action plan for Europe, COM(2009) 278, Brussels, 18.6.2009.

12 See footnote 2

13 See the examples provided in WP 105, section 3.3.

14 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

Unfortunately, despite this premise, **the proposed framework** does not follow through with this concern and **fails to explicitly invite the RFID operator to assess privacy and data protection issues that could arise when tags are carried by individuals in everyday life.** It is not sufficient to consider "*whether the location of Individuals or Users will be monitored through the RFID application*[15]*"*. It is also crucial to analyze the risk of unauthorized monitoring beyond the perimeter of the application. The Framework also fails to describe the steps taken to address these risks. **The Working Party urges the industry to fully address this issue, by clearly mentioning it in the framework as part of a revised risk assessment approach.**

2.3 RFID in the retail sector

One of the key areas of application where tags could end up being carried by individuals is the retail sector. The RFID Recommendation recognized this sector as critical and has addressed it through specific points.

Point 11 of the RFID Recommendation specifically indicates that "*Retailers should deactivate or remove at the point of sale tags used in their application unless consumers […] give their consent to keep tags operational.*

Point 12, allows an exception to this rule by stating that "*Point 11 should not apply if the privacy and data protection impact assessment concludes that tags that are used in a retail application and would remain operational after the point of sale do not represent a likely threat to privacy or the protection of personal data."* This means that deactivation at the point of sale is the default behaviour, unless the PIA concludes otherwise.

However, section D of the proposed PIA Framework only offers two possible conclusions to a PIA Report: the RFID application is either "*Ready for deployment*" or "*Not ready for deployment*", without providing any possibility for an RFID operator to express a conclusion regarding the use of tags beyond the point of sale in retail applications, as required in the RFID Recommendation. The Working Party notes that some applications may justify or require that some tags remain active beyond the point of sale in the retail sector, for specific purposes. Yet the absence of such consideration in the Proposed Framework thus seems to imply that all tags will be deactivated at the point of sale.

More generally, the Working Party observes that the binary choice offered in section D of the PIA framework seems unnecessarily restrictive for RFID Operators, and the RFID industry as a whole. Some application may be considered as "ready for deployment under certain conditions" that would need to be outlined in the conclusion of the PIA Report.

The Working Party invites the authors of the proposed Framework to clarify the issue of tag deactivation in the retail sector. The proposed framework must explicitly require an RFID Operator to address point 12 of the RFID Recommendation in the PIA Report that will be produced (for retail sector applications). **More generally, a revised risk assessment approach should provide the right tools to reach a conclusion regarding the conditions or deployment of an RFID Application.**

[15] In section 2.3.4 of the proposed framework

2.4 Additional remarks

As highlighted above in section 2.2, if the tag is carried by a person (either a User or an Individual), and if the tag contains a unique ID[16], then by definition the tag contains personal data. Strictly speaking, the definitions of "Level 1 Applications" and "Level 0 applications" presented in section 1.5 thus present a contradiction: in most scenarios, it is not possible to say that the RFID Application *does not* process personal data if tags are carried by Individuals or Users. Hence, under these definitions, most applications would qualify as level 2 applications. **Level 0 or level 1 application would thus only apply in rare cases where tags are carried by persons and yet do not have a unique number**.

The Working Party assumes that the authors of the Framework did not intend to give such a limited scope to level 0 and level 1 applications, and that their definitions were meant to encompass applications that process only one type of personal data, namely the tag unique ID. All level definitions could easily be clarified to remove any ambiguity. In any case, the proper definition of a risk assessment based methodology, might result in a rewording of these definitions as well.

The Working Party notes that the Framework refers to tags "*possessed*" by Users or Individuals. This word is too restrictive and should be replaces by "carried", which covers much more appropriately the risk scenarios at hand.

The Working Party believes that the PIA process proposed in the framework should include a stakeholder consultation phase. This involves consulting interested parties (groups, unions, associations …) that can be affected by the RFID application, and exchanging ideas, suggestions and improvements that will allow the application to be deployed in an open and privacy friendly manner, benefiting both the RIFD Operator and the affected Users or Individuals. Such a stakeholder consultation phase clearly contributes to "*information and transparency on RFID use*" as well as the "*awareness raising actions*" envisioned the RFID Recommendation.

The Working Party also highlights that special categories of data[17] require specific conditions to be processed lawfully and securely. The Framework should provide stronger guidance to the RFID Operator on the specific issues related to the processing special categories of data. Identifying the use of special categories of data should also be part of any risk assessment process.

The Framework should also provide RFID operators with guidance regarding the most appropriate time and conditions to conduct a PIA in the development cycle of a RFID product, in order to truly encourage "*security and privacy by design*" as supported by the Recommendation.

---

16 We refer broadly to the "tag ID" to cover any unique identification number (or serial number) that can be accessed in the RFID tag and that allow to uniquely characterize a RFID tag in a certain context.

17 Article 8 of Directive 95/46/EC.

3 Conclusion

Because of the issues highlighted in this Opinion, in particular the absence of a clear and comprehensive privacy and data protection risk assessment approach in the proposed framework, **the Working Party does not endorse the proposed document in its current form.**

It should be highlighted that the inclusion of a proper risk assessment process can clearly facilitate dealing with most of the other issues that have been identified in this opinion. Indeed, if an RFID operator is required to conduct a risk assessment, he would notably identify risks associated with the unauthorized monitoring of RFID tags carried by persons. Furthermore, in the retail sector, it could help present a clear case to show that certain RFID tags (used in a specific application) that *"remain operational after the point of sale do not represent a likely threat to privacy or the protection of personal data"*.

The Working Party is confident that the industry can propose an improved framework based on the comments that have been highlighted in this opinion and is committed to pursuing every relevant route to further improve the proposed Framework and lead to its rapid endorsement.

Done at Brussels, on 13 July 2010

For the Working Party
The Chairman
Jacob KOHNSTAMM