ARTICLE 29 DATA PROTECTION WORKING PARTY

00327/11/EN
WP 180

Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications

Adopted on 11 February 2011

Table of Contents

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure,

has adopted the following opinion:

1 Context

1.1 Introduction

This opinion is a follow-up to opinion[1] 5/2010 (WP 175) on *the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*. While this introduction will repeat some elements of context necessary to understand the purpose and the scope of this new opinion, the reader is invited to consult opinion 5/2010 for further details.

On May 12th 2009, the European Commission issued a recommendation[2] on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. This recommendation invited member states to ensure that *the industry, in collaboration with relevant stakeholders,* develops *a framework for privacy and data protection impact assessment*, which was destined to be submitted for *endorsement to the Article 29 Data Protection Working Party*. 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.

On March 31st 2010, industry representatives delivered a Privacy and data protection Impact Assessment Framework proposal to Working Party 29 for endorsement. However, while this proposal presented a good starting point, it didn't gain the full support of the Working Party, notably because of 3 critical elements that were missing in the proposed framework:

1) A clearly defined risk assessment approach.

2) Consideration for RFID tags carried by persons beyond the operational perimeter of the application.

---

1 Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 175, July 13, 2010.

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

3) A way to explicitly address the tag deactivation principles in the retail sector that are established in the European Commission's Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

On July 13th 2010, the Working Party summarized these elements, as well as other concerns, in Opinion 5/2010, inviting the industry to propose a revised Privacy and data protection Impact Assessment Framework. With regards to the risk assessment component, the Working Party strongly encouraged the industry to build upon existing expertise that the European Network and Information Security Agency (ENISA) could provide in this area.

That same month, ENISA published an independent opinion[3] with practical recommendations to improve the proposed Framework. ENISA's opinion proposed in particular some initial guidelines for the adoption of a comprehensive and recognized methodological risk assessment approach, and suggested several structural improvements.

In the following months, the industry redrafted a revised PIA Framework, taking into account the input provided both by the Working Party and ENISA. On January 12, 2011, this revised PIA Framework was submitted for endorsement *to the Article 29 Data Protection Working Party*.

This opinion formalizes the response of the Working Party to this new 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 "Revised Framework" or simply "Framework" shall refer to the RFID Application Privacy and Data Protection Impact Assessment Framework, transmitted to Working Party 29 on January 12, 2011 and reproduced in the Appendix of this opinion.

1.2 Summary of the Revised Framework

The Revised Framework begins with a review of important internal procedures that are relevant to the execution of a PIA such as: scheduling and reviewing the PIA, compiling relevant documentation, determining relevant persons in the organization to support the PIA process, identifying conditions which might trigger a revision of the PIA in the future and stakeholder consultation.

The PIA process is constructed in two phases:

I. A pre-assessment phase that classifies an RFID application according to a 4 level scale, based on a decision tree. The result of this evaluation allows to determine if a PIA is required or not, and to choose between a "Full Scale PIA" and a "Small Scale PIA". Applications that use RFID tags that are likely to be carried by individuals will require at least a "Small Scale PIA" (level 1), while applications which further process personal data will require a "full scale PIA" (level 2 and 3). Conversely, applications that do not use tags that are likely to be carried by individuals and do not further process personnel data are not subject to a PIA (level 0).

[3] http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia, ENISA Opinion on *the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* of March 31, 2010.

II. A risk assessment phase that is broken down in 4 main steps:
    1) Characterization of the application (data types, data flows, RFID technology, data storage and transfers, etc.)
    2) Identification of the risks to personal data, by evaluating threats, their likelihood and their impact in terms of privacy and compliance with European legislation.
    3) Identification and recommendation of controls, in response to previously identified risks.
    4) Documentation of the results of the PIA, establishment of a resolution regarding the conditions of implementation of the RFID application under review, and information concerning residual risks.

Each step in the risk assessment phase is further supported by elements provided in the Annexes of the Revised Framework and designed to provide guidance to the reviewer with:

- A template to describe key characteristics of the RFID application.
- A list of 9 privacy targets for the RFID Application, derived from Directive 95/46/EC.
- A list of typical privacy risks, with descriptions and examples.
- A list of examples of controls and mitigating measures that can be used in response to previously identified risks.

The result of a PIA is formalized by the RFID application operator in a PIA report, which describes the RFID application and documents the details of the 4 risk assessment steps referred above.

2 Analysis

The Working Party acknowledges the depth of the work that the industry associations and experts, academics, and individual companies have invested in producing a Revised Framework in the past months. The authors of the Framework took the opportunity of this revision not only to address most concerns highlighted by the Working Party but also to present a clarified structure and stronger guidelines for the RFID operators who will implement this Framework.

The Working Party notes that the Revised Framework is based on a risk management approach, and reiterates that this is an essential component of any Privacy and Data Protection Impact Assessment Framework.

The working party also welcomes the explicit inclusion of a stakeholder consultation process as part of the internal procedures needed to support the execution of a PIA.

The proposed risk assessment methodology is initiated by a pre-assessment decision tree that classifies RFID applications according to 4 levels. The Working Party observes that the proposed decision tree contains an ambiguity with regard to what may or may not be considered as personal data in an RFID Application. If a tag containing a unique ID is destined to be carried by a person, then the tag ID should be considered as personal data, as previously highlighted in Opinion 5/2010. Thus, in most scenarios, if the tag is destined to be carried by a person it would qualify as a level 2 application and not a level 1 application as

suggested by the Framework. Nevertheless, the Working Party welcomes the fact that the revised Framework clearly requires RFID Operators to conduct a PIA whenever tags are carried by an individual.

As described in several previous opinions[4], one of the main privacy concerns related to RFID technology "*arises from uses of RFID technology which entail individual tracking and obtaining access to personal data"*. While an RFID Operator may not have such a goal in mind when deploying an RFID Application, it is important to consider the risk that a third party may use tags for such unintended purposes. The revised framework now clearly requires RFID Operators to evaluate the risks that may arise when tags may be used outside the operational perimeter of an RFID application and/or are carried by persons.

This concern has received particular attention in the retail sector, where it is feared that tagged items bought by individuals could be misused by retailers or third parties for tracking or profiling purposes. The European Commission addressed this concern in the Recommendation by establishing the principle that tags must be deactivated at the point of sale unless the customers give their informed consent to keep tags operational. The same Recommendation allows an exception to this deactivation principle if the PIA concludes that keeping tags operational after the point of sale does not represent *a likely threat to privacy or the protection of personal data*. The Working Party observes that a risk management approach, as suggested by the Framework, is an essential tool for the RFID Operator to assess the risks of taking the responsibility to keep tags activated after the point of sale.

Conducting a PIA will result in the production of a PIA report that should be made available to the competent authority at least 6 weeks before the deployment of the RFID Application. The Working Party wishes to highlight that conducting a PIA will also require the RFID Operator to *develop and publish a concise, accurate and easy to understand information policy for each of their applications* (as described in point 7 of the Recommendation). This information policy should notably include *a summary of the Privacy and data protection Impact Assessment*.

As this Framework begins to be implemented on concrete RFID Applications, its content will likely require adjustments, which can only be informed through experience and feedback from all stakeholders, including the industry, consumers, data protection authorities and ENISA. This will likely notably be the case regarding the distinction between a "full scale" or a "small scale" PIA, as defined in the Revised Framework. Additionally, according to the Recommendation, the European Commission is expected to provide *a report on the implementation of the Recommendation, its effectiveness and its impact on operators and consumers*, with regards in particular to measures concerning the retail sector. This report is set to be produced 3 years after the Recommendation was published, that is by May 2012. However, considering that the Framework may take 6 months to fully take effect, supplementary time would be beneficial for all stakeholders before such an evaluation is conducted. Therefore, the Working Party would like to suggest to the European Commission to either postpone or supplement the proposed report at a later date set in 3 years from the publication of this opinion.

[4] See for example opinion 5/2010 (WP 175) and WP 105, "*Working document on data protection issues related to RFID technology*", January 19, 2005.

3 Conclusion

The Working Party endorses the Revised Framework submitted on January 12, 2011. This framework shall take effect no later than 6 months after the publication of this opinion.

A PIA is a tool designed to promote “privacy by design”, better information to individuals as well as transparency and dialogue with competent authorities. Consequently, since some RFID Applications will be implemented in several member states, it is important that PIA reports are translated and made available to competent authorities in their national language.

The Working Party will continue to support future dialogue with the industry, with regards to providing enhancements and clarifications in the structure and implementation of the RFID PIA Framework, as informed by experience and feedback from all stakeholders.