RFID Privacy Impact Assessment Framework
From promise to reality: steps to successful implementation

Gérald Santucci
Head of Unit
INFSO D4, European Commission

Berlin
November 25th, 2011
From RFID Recommendation to PIA Framework

Framework on privacy impact assessments and information security

A framework on privacy impact assessments should be developed at Community level within 12 months from the publication of this Recommendation in the Official Journal of the European Union.

This framework should be endorsed by the Article 29 Data Protection Working Party.

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

11 February 2011

6 April 2011

Neelie Kroes
Vice-President of the European Commission
The “decision tree” guides the initial analysis to determine the scope of the PIA

Q2: Does the RFID Application process personal data? OR Will the RFID Application link RFID data to personal data?

- yes
- no

Q2a: Do the RFID tags used in the RFID Application contain personal data?

- yes
- no

- Level 3
- Level 2

Q2b: Is it likely that the RFID tags you process are carried by an individual?

- yes
- no

- Level 1
- Level 0

- Full Scale PIA
- Small Scale PIA
- No PIA

“Personal Data” as defined by the Directive 95/46/EC (Article 2) shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

A “RFID Application” is a system that processes data through the use of tags and readers and which is supported by and is part of a back-end system and a networked communication infrastructure.
The Risk Assessment Methodology

Risk Assessment Methodology for RFID as outline in the PIA Framework
The virtues of the PIA approach

- PIA automatically ensures legal compliance for industry with the EU Data Protection Directive.

- Global scalability is feasible if regions take their local privacy legislation or practices as privacy targets.

- The methodology can be translated into and facilitated by a technical tool.
  - e.g. GS1 PIA Tool (November 2011)

- The methodology is independent of any application, industry, sector, or even technology.
The challenges of the PIA approach

- Lack of awareness
  - In EU countries
  - In companies

- Lack of formal standardisation
  - Mandate M/436 2nd phase

- High degree of genericity
  - But also high degree of adaptability
  - From “general framework” to “sectorial templates”

- Self- and co-regulation vs. legislation?
The Commission will organise **a conference in Brussels on 8th February 2012** to consolidate the results of ongoing national consultations and reach consensus on a common European approach PIA Framework implementation.

The PIA Framework is part of the context of other information assurance, data management, and operational standards that provide good data governance tools for RFID and other Applications. The current Framework could be used as a basis for the development of industry-based, sector-based, and/or application-based PIA templates. As in the implementation of any theoretical document, the PIA Framework may require clarification of its application of terms, as well as guidance on practices that should be based on practical experience, that may help in its implementation.

**PIA Templates** may be developed based on the Framework to provide industry-based, application-based, or other specific formats for PIAs and resulting PIA Reports.
The Privacy Impact Assessment Framework for RFID Applications

PIA FRAMEWORK (12 January 2011)

1) ORIGINAL TEXT

- The "Privacy Impact Assessment Framework for RFID applications" has been endorsed by the Article 29 Working Party on 11 February 2011 successfully completing a task that started nearly two years ago.

2) TRANSLATIONS

- This document is also available in the official EU languages BG, ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV from this page.

OPINION OF THE A29WP (11 February 2011)


SIGNING CEREMONY (6 April 2011)

PRESS RELEASE OF THE EUROPEAN COMMISSION
PRESS RELEASES OF SOME STAKEHOLDERS
CONCLUSION

The RFID PIA Framework marks the success of a co-regulatory approach to manage potential privacy risks.

Companies are encouraged to adopt the methodology and embed privacy into the design of their systems.