The Recommended RFID Privacy and Data Protection Impact Assessment Framework in the EU

Nikita Maria, PhD Candidate
Department of Applied Informatics
University of Macedonia, Thessaloniki, Greece
nikita_ma@yahoo.gr

Abstract

Nowadays, the RFID technology can be found in different sectors and implemented in a big number of applications and it is commonly accepted that its use has offered powerful benefits to its adopters. But, it has also caused intense reactions and privacy debates. In many cases privacy is set in danger because of its ability to process and transfer data wirelessly, even without line of sight.

It is a challenging technology for the privacy regulation and the regulators must be vigilant. Since 2005, significant actions have taken place that lead to the technology's safe implementation. The European Commission and the Article 29 Data Protection Working Party in collaboration with interested parties, including manufacturers and deployers of the RFID technology as well as with privacy advocates, published a series of working documents and opinions and resulted in developing a Privacy and Data Protection Impact Assessment Framework.

This paper focuses on the steps that have been done until today for the safe implementation of the RFID systems and especially to the final Revised PIA Framework that was recommended and endorsed.

1. Introduction

"Privacy, like the weather, is something everyone talks about. But unlike the weather, there is much that should do, and can, be done about it", Marx G.T. fairly commented [Marx G.T., 2012, pp.5]. As the years are passing and the information technologies are becoming part of our everyday life, privacy has become a major issue that everyone worries about it. Especially the last decade, consumers have showed big interest and growing concern about their privacy and the protection of their personal data. The rapid evolution and changes of the information technologies are very challenging for the privacy regulation.

The RFID technology is one of these challenging technologies that may intrude into our life and our privacy. This technology is using a micro-chip that can be attached to any object, animal or even a person and offers the ability to collect information about it wirelessly and without line of sight. It has the potential to benefit Europeans in many ways, such as safety, convenience, accuracy and accessibility [Commission's Communication, 2007]. Until today, it has been used in different sectors and a variety of applications with an impact on the lives of Europeans. Some of these applications, randomly referred, are healthcare, logistics, transportation, payment systems, security and physical access control systems, animal tracking, human profiling and tracking,

official documents management (passports, IDs), supply chain management and retail management. All these applications, and even more, offer powerful economic and societal benefits to their adopters.

But at the same time the widespread use of the RFID technology has caused intense reactions too. As Spiekermann S. notes [pp.2, 2011], the reason why the RFID technology has caused strong privacy debates, intense reactions and even fear, is threefold. Firstly, the invisibility of the technology is a major factor that raises consumer fear. The RFID chip is very small in some cases or it is hidden and cannot be easily seen by the consumer and the data are transmitted wirelessly and even from long distance and without line of sight. Secondly, unlike other devices, such as the mobile phones, the RFID chip cannot be turned off by the consumer. And finally, it is expected to be embedded in all the products that we use in our everyday life.

The Article 29 Data Protection Working Party has showed great concern about the possible violation of human dignity and data protection rights because of the extensive and mindless use of the RFID technology. In the next chapters, the steps that have been done from the European Commission and the Article 29 Data Protection Working Party until today for the safe implementation of the RFID systems are presented. Moreover, more emphasis is given to the Revised Privacy and Data Protection Impact Assessment Framework for RFID Applications that was proposed and endorsed by the Article 29 Data Protection Working Party.

2. Steps EU has done towards the safe implementation of the RFID systems

The European Commission and the Article 29 Data Protection Working Party (hereafter Art. 29 WP) have played an important role in the steps that have been done until today for the safe implementation of the RFID systems.

In 2005, the Art. 29 WP consulted with interested parties, including manufacturers and deployers of the RFID technology as well as with privacy advocates, made a first assessment and adopted a working document on data protection issues related to RFID technology [Art. 29 WP, 2005a]. The purpose of this working document was twofold. Firstly, its purpose was to provide guidance to RFID deployers on the application of the basic principles set out in EC Directives [95/46/EC and 2002/58/EC] because they are responsible for the personal data gathered and they have to comply with the data protection principles. And secondly, to provide guidance to technology's manufacturers and standardization bodies on their responsibility towards designing privacy compliant technology and ensure that the deployers will be able to carry out their obligations under the data protection Directive. This working document was only an initial attempt. The Working Party decided to put it up for public consultation (31/03/2005) and continued working on the issue.

A summary of the results of the public consultation on Art. 29 Working Document 105 on Data Protection Issues Related to RFID technology was presented in the document WP 111 [Art. 29 WP, 2005b]. The results showed that some of the responses consider the paper positively while others are more critical of certain conclusions. Some consider that the Directive adequately covers the privacy and data protection issues and plead for self-regulation to complement the data protection

Directive, while others suggest complementing the data protection Directive with specific rules for RFID.

After two years, in 2007, the Commission of the European Communities, based on these results, presented a communication [European Commission, 2007] and proposed the next steps that must be done to overcome the barriers from the implementation of the RFID. With the communication the Commission addressed the need for a legal and policy framework to protect privacy and to make the technology acceptable to the consumers. The same year, an RFID Expert Group on Radio Frequency Identification was created [European Commission, 2007] in order to provide advice and objective information to the Commission on different issues related to the deployment of RFID, develop guidelines on how RFID applications should operate and support the Commission's efforts to promote awareness about the RFID technology.

In 2009, Viviane Reding, European Union's Commissioner for Information Society and Media, warned that RFID would only realize their economic potential "*if they are used by the consumer and not on the consumer. No European should carry a chip in one of their possessions without being informed precisely what they are used for, with the choice to remove or switch it off at any time*" [EU Commissioner Reding, 2009].

The same year the Commission published a Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification [European Commission, 2009]. This Recommendation was an attempt to provide guidance to Member States on the design and operation of RFID applications and on measures to be taken for the deployment of the applications to ensure that national legislation is respected. Further, with this Recommendation the Commission called Member States to ensure that industry will develop a framework for privacy and data protection impact assessments, in collaboration with relevant civil society stakeholders, and submit it for endorsement to the Art. 29 WP. According to Clarke R. [2009] "*a privacy impact assessment is a systematic process for evaluating the potential effects on privacy of a proposed system* [..]".

After that, based on the Recommendation, an Industry Proposal on Privacy and Data Protection Impact Assessment Framework for RFID Applications [Industry Proposal, 2010] was formed by an informal RFID workgroup led by industry representatives. The purpose of the proposed Framework was to help the RFID Application Operators to conduct a PIA on their applications and to develop a common structure of the PIA analysis and Reports that result from such PIAs. In addition, the Framework provided a basis for the development of sector-specific PIA Templates.

The proposed Framework was submitted to the Art. 29 WP for endorsement, as the Recommendation required, but it didn't meet its expectations and the Art. 29 WP didn't endorse it in its current form. Instead, it identified three critical concerns that should be taken into account: a risk assessment was absent, privacy and data protection issues when tags are carried by individuals in everyday life weren't estimated and tag deactivation or removal in the retail sector wasn't clarified. So, the Working Party suggested that the industry should propose another Framework, improved and based on the comments and the remarks that have been highlighted at the Opinion 5/2010 [Art. 29 WP, 2010]. Also, ENISA published an independent

opinion [ENISA, 2010] with some useful and practical recommendations for improvement.

The industry representatives took into account the recommendations provided both by the Working Party and ENISA and formed a revised PIA Framework [Industry Proposal, 2011] and submitted it for endorsement to the Working Party. The Working Party in its opinion [Art. 29 WP, 2011] noted that the Revised Framework meets its expectations and entails a risk assessment phase, as it was recommended. Thus, the Revised Framework was endorsed by the Working Party with one remark: that the PIA Reports have to be translated to each competent authority's national language. This Revised PIA Framework is analytically presented to the next chapter.

3. The Revised Privacy and Data Protection Impact Assessment Framework for RFID Applications

The Revised Privacy and Data Protection Impact Assessment Framework for RFID Applications was published in 2011, after the Commission's Recommendation [European Commission, 2009] for developing such a framework. The main purpose of this Framework, as has already been discussed, is to provide guidance to RFID application operators for conducting a PIA on their applications and set a common structure for the Reports.

The PIA process is recommended to be conducted at an early stage of the design or upgrade of the application. Otherwise it may be very difficult and more expensive for the operators to make any adjustments and changes to conduct the PIA.

Figure 1 Process phases of a privacy impact assessment for RFID [Wright D. & De Hert P., 2012]

The proposed PIA has two main phases, the initial analysis phase and the privacy risk assessment phase and at the same time documentation and reporting are necessary (Figure 1). Before the implementation of the PIA process the operator has to do some internal procedures to support the execution of the PIA. And as Spiekermann S. [2011] notes, some key points also are necessary to be considered before engaging in a PIA, such as who should the RFID operator be, what the scope of the application is and when the right time to conduct the PIA is.

At the initial analysis phase, the pre-assessment phase, the operator has to determine whether a PIA is needed or not and to what extent with the help of a decision tree (Figure 2). The degree to which each application entails privacy risks (or not) is different and therefore it is important at the initial analysis phase to make it clear whether the application leads to profiling, links to personal data, processes personal data or contains personal data. In every case it is being treated differently.

According to the proposed decision tree, the main question that the operator has to answer is if the RFID application processes personal data or RFID data links to personal data (Q1). If the application doesn't process any personal data or the RFID data doesn't link to personal data (Q2b) and the RFID tags are not carried by an individual, then it is a Level 0 application where there is no risk, no privacy problems will ever arise and therefore is not required to conduct a PIA. But, in case there is likelihood that the RFID tags may be carried by individuals and probably used for profiling, it is a Level 1 application where the risk is low and it is required to conduct a simple Small Scale PIA.

In other cases, where the application processes personal data or links to personal data, either it is a Level 2 application where the RFID tags do not contain personal data or it is a Level 3 application where the tags contain personal data (Q2a). In both cases, since personal data is processed, a more complex Full Scale PIA with a highly detailed privacy risk assessment is required to identify the privacy risks and ensure that they are well worked out. The main difference between Level 2 and Level 3 applications is the mitigation strategies adopted because they deal with different risk environments.

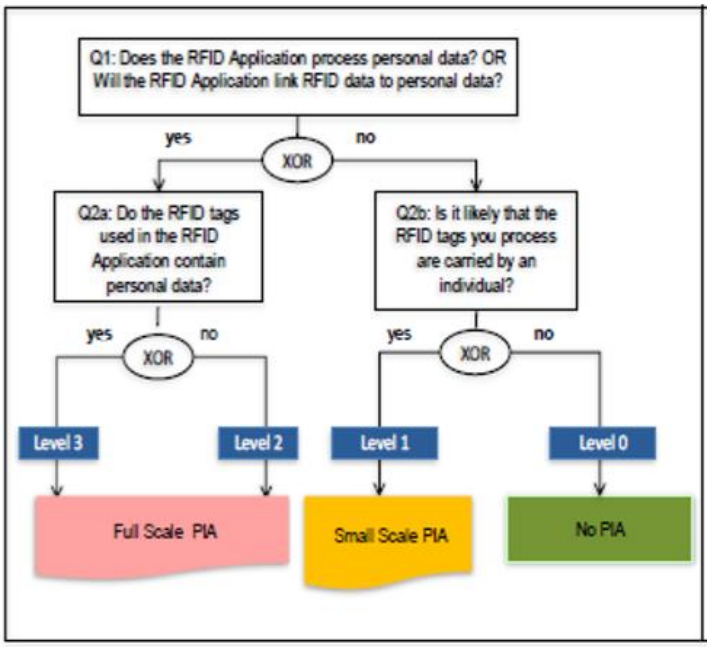

Figure 2 Decision tree on whether and at what level of detail to conduct a PIA [Industry Proposal, 2011, pp. 7].

At the risk assessment phase, the privacy risks are identified. Particularly, their probability of occurrence and the size of their effects are considered and ways to proactively moderate them are planned in detail. It is important the privacy risks to be identified before any final decisions concerning the application's architecture are taken, so that mitigation strategies will be easily embedded into the system's design. Otherwise radical changes may need to be done and the implementation cost will be much higher.

At the table below, the nine privacy targets (P1-P9) as defined in the European Data Protection Directive 95/46/EC [Chapter II, Sections I to IX] and concrete sub-targets

as defined in the Privacy Impact Assessment Guideline for RFID Applications [Oetzel et al., 2011] are presented. The operators can use this list at the risk assessment phase to identify the privacy risks that may occur to their applications and that need to be mitigated.

Privacy targets as defined in the PIA Framework (Annex II)		**Privacy target code and name**		**Description of privacy target**
P1	Safeguard of quality of personal data	P1.1	Ensuring fair and lawful processing through transparency[7]	E.g. providing a description of the data processing activities required for product and service delivery, ensuring internal and external transparency. See Directive 95/46/EC, Section I, Article 6 (a).
		P1.2	Providing purpose specification and limitation	See Directive 95/46/EC, Section I, Article 6 (b).
		P1.3	Ensuring data avoidance and minimisation	e.g. processing only adequate and relevant personal information, non-excessive use of personal data. See Directive 95/46/EC, Section I, Article 6 (c).
		P1.4	Ensuring quality of data	E. g. ensuring accuracy, up-to-dateness, erasure or rectification of data that is incorrect or incomplete. See Directive 95/46/EC, Section I, Article 6 (d).
(P9)	Safeguard of quality of personal data AND Compliance with data retention requirements	P1.5	Ensuring limited duration of data storage	E.g. ensuring that data permitting identification of the data subject is not stored longer than necessary. See Directive 95/46/EC, Section I, Article 6 (e).
P2	Legitimacy of processing personal data	P2.1	Legitimacy of processing personal data	E.g. ensuring that consent, contract, etc. is available. See Directive 95/46/EC, Section II, Article 7 (a-f).
P3	Legitimacy of processing sensitive personal data	P3.1	Legitimacy of processing sensitive personal data	E.g. ensuring that explicit consent from the data subject, a special legal basis, etc. is available. See Directive 95/46/EC, Section III, Article 8.
P4	Compliance with the data subject's right to be informed[8]	P4.1	Providing adequate information in cases of direct collection of data from the data subject	E.g. providing information about: identity of the controller, purpose of processing, recipients of the data, etc. See Directive 95/46/EC, Section IV, Article 10 (a-c).
		P4.2	Providing adequate information where the data has not been obtained directly from the data subject	E.g. providing information about: identity of the controller, purpose of processing, categories of data concerned, recipients of the data, etc. See Directive 95/46/EC, Section IV, Article 11.

P5	Compliance with the data subject's right to access, correct and erase data	P5.1	Facilitating the provision of information about processed data and purpose	See Directive 95/46/EC, Section V, Article 12 (a).
		P5.2	Facilitating the rectification, erasure or blocking of data	See Directive 95/46/EC, Section V, Article 12 (b).
		P5.3	Facilitating the notification to third parties about rectification, erasure and blocking of data	See Directive 95/46/EC, Section V, Article 12 (c).
P6	Compliance with the data subject's right to object	P6.1	Facilitating the objection to the processing of personal data, direct marketing activities and disclosure of data to third parties	E.g. providing information before disclosure to third parties and/or use of personal data or direct marketing, so that objection is possible. See Directive 95/46/EC, Section VII, Article 14.
		P6.2	Facilitating the objection to being subject to decisions that are solely based on automated processing of data	See Directive 95/46/EC, Section VII, Article 15.
P7	Safeguard of confidentiality and security of processing	P7.1	Safeguarding confidentiality and security of processing	***Here, security targets, which are defined in BSI's technical guidelines TG 03126, are relevant.*** See Directive 95/46/EC, Section VIII, Articles 16 and 17.
P8	Compliance with notification requirements	P8.1	Compliance with notification requirements	See Directive 95/46/EC, Section IX, Articles 18 to 21.

Table 1 Privacy targets according to the EU Data Protection Directive 95/46/EC [Oetzel M.C, Spiekermann S., Grüning I., Kelter H. and Mull S. (2011), Privacy Impact Assessment Guideline for RFID Applications, pp. 19-21].

A privacy risk assessment methodology is actually using a process reference model that has generic functionality and ensures that privacy risks and mitigation strategies are identified. The PIA process reference model has been visualized in the PIA Framework and it consists of four key steps (Figure 3).

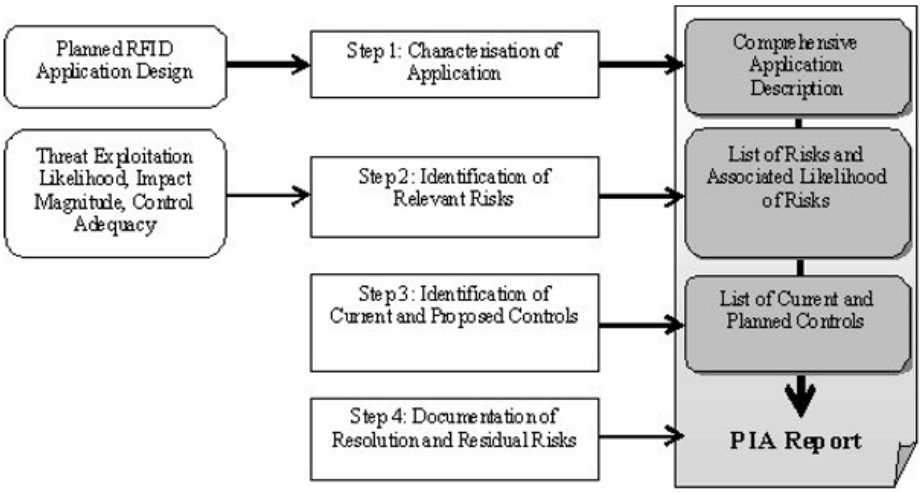

Figure 3 PIA process reference model [Industry Proposal, 2011, pp.8]

The first step is the application characterization. At this step, data flow diagrams have to be created to visualize how the information flows in the application. Also, a description of the application's environment is necessary to give a complete and comprehensive picture of the application. In the PIA Framework [Industry Proposal, 2011, Annex I, pp. 12] the operator can find a reference about the information that has to include in the PIA Report for this step.

The second step involves the identification of relevant risks. The operators can use the nine privacy targets as defined in EU Directive 95/46/EC [Chapter II, Sections I to IX, Table 1] as a guide to identify threatening situations. Also, a list of privacy risks that may affect the ability to meet the privacy targets is presented in Annex III of the PIA Framework [Industry Proposal, 2011, pp. 14-16] and can be used by the operators. Not all risks are likely to occur, so the operator has to specify the likelihood of occurrence, their significance and the magnitude of their impact.

At the third step, the operators should find mitigation strategies for each risk they have identified at the previous step. The operators should recommend controls for implementation to minimize, mitigate or eliminate the identified privacy risks. These controls can be either technical if they are associated with the application's architecture (e.g. authentication mechanisms) or nontechnical if they are associated with the management. Also, the controls can be either preventive if they suspend any violation attempts or detective if they warn for violation attempts. Examples of such controls can be found at the Annex IV of the PIA Framework [Industry Proposal, pp. 17-20].

Finally, the fourth step is the Reporting and is reached after the risk assessment is completed. The final resolution and any remarks about controls and residual risks are documented at this step. The PIA Report results from the PIA process, includes a comprehensive description of the technology and documentation of the four steps and is given to the competent authorities. Each member state has to decide if the Report will be given upon request or not.

An RFID Application is characterized as approved since the PIA process is completed successfully. This means that all the relevant risks are identified and mitigation strategies are designed to assure that all the privacy risks are minimized. If the RFID Application is not approved, this means that it doesn't meet the requirements of compliance and a corrective action plan should be applied and then a new PIA should be conducted.

4. Conclusions and Recommendations

Privacy issues have existed since the information technologies were first introduced. The opposition for RFID technology lies to its automatic management of data wirelessly, without prior information of the consumer.

The RFID technology is very challenging for the privacy regulation and the regulators must be vigilant. Although it offers powerful economic and societal benefits to its adopters, it also constitutes a great threat to privacy. It is clear that the RFID applications must be "socially and politically acceptable, ethically admissible and legally allowable" [Commission's Communication, 2007], so as to be able to take full

advantage of their benefits without any impact. For these reasons, the European Commission and the Article 29 Working Party took action to restrict the technology's pervasiveness and protect privacy.

The European Commission and the Article 29 Data Protection Working Party played a key role throughout the entire process for the safe implementation of the RFID systems. The Commission addressed the need for developing a legal and policy framework for privacy and data protection impact assessments (PIA Framework) to protect privacy and to make the technology acceptable to the consumers, and then submit it for endorsement to the Article 29 Working Party.

Two attempts were made for developing a PIA Framework. The first was in 2010, but it took a negative answer from the Article 29 Working Party. The second attempt was made a year after, where the RFID workgroup proposed a Revised PIA Framework taking into account all the recommendations for improvement. This Revised PIA Framework was endorsed by the Article 29 Working Party and was even characterized as "*a first-of-its-kind milestone in Europe* [..]. *It effectively creates a win-win situation for business and consumers*", by Neelie Kroes, the Vice-President of the European Commission for the digital agenda, at one of his speeches [SPEECH/11/236, 2011].

The Revised PIA Framework fully complies with the EU data protection legislation and the Commission recommended its use, but it didn't make it mandatory. However, the operators still have to comply with the basic privacy principles and the data protection law, so the use of the PIA Framework could be a good guide which will facilitate the compliance with the regulatory framework.

According to Art. 29 WP, in Opinion 9/2011, after the implementation of the PIA Framework on concrete RFID Applications and based on practical experience and feedback, it will be easier to specify the Framework's effectiveness and impact on operators and consumers. In this way, necessary adjustments will be identified and with appropriate and corrective actions, the PIA Framework will become a useful tool that contributes to a high level of trust and compliance with the national regulatory framework. Thus, regulation will no more be an obstacle to the technology's evolution and adoption; it won't limit its widespread deployment and it will be feasible to fully exploit the technology's powerful benefits.

Furthermore, the Revised PIA Framework for RFID could be a good example for other technological fields too. It can be adaptable to other technologies or it can be a starting point for implementing sector-specific PIA templates.

To conclude, the proposed PIA Framework seems to be a good solution for the safe implementation of the RFID systems. Privacy risks and data protection issues are fully addressed and consumer's trust is gained little by little. However, it is recommended at first to be implemented by a significant number of industries and its impact to be carefully monitored.

5. References

Article 29 Data Protection Working Party (2005), Working document on data protection issues related to RFID technology (WP 105) published on 19 January 2005, online at
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf
[accessed 22.03.2014].

Article 29 Data Protection Working Party (2005), Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology Adopted on 28 September 2005, online at
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp111_en.pdf
[accessed 22.03.2014].

Article 29 Data Protection Working Party (2010), Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, online at
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf
[accessed 22.03.2014].

Article 29 Data Protection Working Party (2011), Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, online at
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
[accessed 22.03.2014].

Clarke, R. (2009), Privacy impact assessment: Its origins and development, Computer law & security review, 25(2), 123-135.

ENISA (2010), Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, online at http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia [accessed 22.03.2014].

European Commission (2007), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:en:PDF
[accessed 22.03.2014].

European Commission Decision (2007), Setting up the Expert Group on Radio Frequency Identification (2007/467/EC), online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:0030:EN:PDF
[accessed 22.03.2014].

European Commission (2009), Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, online at http://ec.europa.eu/smart-

regulation/impact/ia_carried_out/docs/ia_2009/c_2009_3200_en.pdf [accessed 22.03.2014].

EU Commissioner Reding (2009), Citizens' privacy must become priority in digital age (IP/09/57), online at http://europa.eu/rapid/press-release_IP-09-571_en.htm?locale=en [accessed 22.03.2014].

EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EU Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Industry Proposal (2010), Industry Proposal on Privacy and Data Protection Impact Assessment Framework for RFID Applications (2010), online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf [accessed 22.03.2014].

Industry Proposal (2011), Privacy and Data Protection Impact Assessment Framework for RFID Applications of 12 January 2011 (WP 180), online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf [accessed 22.03.2014].

Kroes N. (2011), Smart tags - working together to protect privacy and Data Protection Impact Assessment Framework Signing Ceremony Brussels, online at http://europa.eu/rapid/press-release_SPEECH-11-236_en.htm [accessed 22.03.2014].

Kumar, R. (2003), Interaction of RFID technology and public policy. In RFID Privacy Workshop.

Oetzel, M.C., Spiekermann, S., Grüning, I., Kelter, H., Mull, S. (2011), Privacy Impact Assessment Guideline, edited by Julian Cantella, online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile [accessed 22.03.2014].

Spiekermann, S. (2012), The RFID PIA–Developed by Industry, Endorsed by Regulators, In Privacy Impact Assessment, Springer Netherlands, 323-346.

Treasury Board Secretariat of Canada (2002), Privacy Impact Assessment Guidelines: A framework to Manage Privacy Risks, online at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld1-eng.asp [accessed 22.03.2014].

Wright, D., and De Hert, P. (2012), Introduction to privacy impact assessment, Springer Netherlands, 3-32.