RECOMMENDATIONS

COMMISSION

COMMISSION RECOMMENDATION

of 12 May 2009

on the implementation of privacy and data protection principles in applications supported by radio-frequency identification

(notified under document number C(2009) 3200)

(2009/387/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Community, and in particular Article 211 thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Radio frequency identification (RFID) marks a new development in the information society where objects equipped with microelectronics that can process data automatically will increasingly become an integral part of every day life.

(2) RFID is progressively becoming more common, and hence a part of individuals' lives in a variety of domains such as logistics [1], healthcare, public transport, the retail trade, in particular for improved product safety and faster product recalls, entertainment, work, road toll management, luggage management, and travel documents.

(3) RFID technology has the potential to become a new motor for growth and jobs and thus make a powerful contribution to the Lisbon Strategy, as it holds great promise in economic terms, where it can bring about new business opportunities, cost reduction and increased efficiency, in particular in tackling counterfeiting and in managing e-waste, hazardous materials, and the recycling of products at their end of life.

(4) RFID technology enables the processing of data, including personal data, over short distances without physical contact or visible interaction between the reader or writer and the tag, such that this interaction can happen without the individual concerned being aware of it.

(5) RFID applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. They can process personal data stored on the tag such as a person's name, birth date or address or biometric data or data connecting a specific RFID item number to personal data stored elsewhere in the system. Furthermore, the potential exists for this technology to be used to monitor individuals through their possession of one or more items that contain an RFID item number.

(6) Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design').

(7) RFID will only be able to deliver its numerous economic and societal benefits if effective measures are in place to safeguard personal data protection, privacy and the associated ethical principles that are central to the debate on public acceptance of RFID.

(8) Member States and stakeholders should, especially in this initial phase of RFID implementation, make further efforts to ensure that RFID applications are monitored and the rights and freedoms of individuals are respected.

[1] COM(2007) 607 final.

(9) The Commission communication of 15 March 2007 'Radio frequency identification (RFID) in Europe: steps towards a policy framework' ([1]) announced that clarification and guidance would be provided on the data protection and privacy aspects of RFID applications through one or more Commission Recommendations.

(10) The rights and obligations concerning the protection of personal data and the free movement of such data, as provided for by 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 ([2]) and 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) ([3]) are fully applicable to the use of RFID applications that process personal data.

(11) The principles laid down in Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity ([4]) should be applied in the development of RFID applications.

(12) The Opinion of the European Data Protection Supervisor ([5]) provides guidance as to how to handle products that contain tags which are provided to individuals and calls for privacy and security impact assessments to identify and develop 'best available techniques' to safeguard the privacy and security of RFID systems.

(13) RFID application operators should take all reasonable steps to ensure that data does not relate to an identified or identifiable natural person through any means likely to be used by either the RFID application operator or any other person, unless such data is processed in compliance with the applicable principles and legal rules on data protection.

(14) The Commission communication of 2 May 2007 'Promoting data protection by privacy enhancing technologies (PETs)' ([6]) sets out clear actions to achieve the goal of minimising the processing of personal data and using anonymous or pseudonymous data wherever possible by supporting the development of PETs and their use by data controllers and individuals.

(15) The Commission communication of 31 May 2006 'A strategy for a secure information society — "Dialogue, partnership and empowerment"' ([7]) acknowledges that diversity, openness, interoperability, usability and competition are key drivers for a secure information society, highlights the role of Member States and public administrations in improving awareness and in promoting good security practices, and invites private-sector stakeholders to take initiatives to work towards affordable security certification schemes for products, processes and services addressing EU-specific needs, in particular with respect to privacy.

(16) The Council Resolution of 22 March 2007 on a strategy for a secure information society in Europe ([8]) invites Member States to give due attention to the need to prevent and fight new and existing security threats to electronic communications networks.

(17) A framework developed at Community level for conducting privacy and data protection impact assessments will ensure that the provisions of this Recommendation are followed coherently across Member States. The development of such 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) ([9]).

(18) The Commission will ensure the development of guidelines at Community level on information security management for RFID applications, building on existing practices and experiences gained in Member States and third countries. Member States should contribute to that process and encourage private entities and public authorities to participate.

(19) An assessment of the privacy and data protection impacts carried by the operator prior to the implementation of an RFID application will provide the information required for appropriate protective measures. Such measures will need to be monitored and reviewed throughout the lifetime of the RFID application.

(20) In the retail trade sector, an assessment of the privacy and data protection impacts of products containing tags which are sold to consumers should provide the necessary information to determine whether there is a likely threat to privacy or the protection of personal data.

([1]) COM(2007) 96 final.
([2]) OJ L 281, 23.11.1995, p. 31.
([3]) OJ L 201, 31.7.2002, p. 37.
([4]) OJ L 91, 7.4.1999, p. 10.
([5]) OJ C 101, 23.4.2008, p. 1.
([6]) COM(2007) 228 final.
([7]) COM(2006) 251 final.
([8]) OJ C 68, 24.3.2007, p. 1.
([9]) Article 2(1) of Regulation (EC) No 460/2004 of the European Parliament and of the Council (OJ L 77, 13.3.2004, p. 1).

(21) 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.

(22) RFID applications with implications for the general public, such as electronic ticketing in public transport, require appropriate protective measures. RFID applications that affect individuals by processing, for example, biometric identification data or health-related data, are especially critical with regard to information security and privacy and therefore require specific attention.

(23) Society as a whole needs to be aware of the obligations and rights that are applicable in relation to the use of RFID applications. The parties that deploy the technology therefore have a responsibility to provide individuals with information on the use of these applications.

(24) Raising awareness among the public and small and medium-sized enterprises (SMEs) about the features and capabilities of RFID will help allow this technology to fulfil its economic promise while at the same time mitigating the risks of it being used to the detriment of the public interest, thus enhancing its acceptability.

(25) The Commission will contribute to the implementation of this Recommendation directly and indirectly by facilitating dialogue and cooperation among stakeholders, in particular through the Competitiveness and Innovation Framework Programme (CIP) established by Decision No 1639/2006/EC of the European Parliament and of the Council [1] and Seventh Framework Research Programme (FP7) established by Decision No 1982/2006/EC of the European Parliament and of the Council [2].

(26) Research and development on low-cost privacy-enhancing technologies and information security technologies is essential at Community level to promote a wider take-up of these technologies under acceptable conditions.

(27) This Recommendation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Recommendation seeks to ensure full respect for private and family life and the protection of personal data,

[1] OJ L 310, 9.11.2006, p. 15.
[2] OJ L 412, 30.12.2006, p. 1.

HEREBY RECOMMENDS:

Scope

1. This Recommendation provides 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.

2. This Recommendation provides guidance on measures to be taken for the deployment of RFID applications to ensure that national legislation implementing Directives 95/46/EC, 1999/5/EC and 2002/58/EC is, where applicable, respected when such applications are deployed.

Definitions

3. For the purposes of this Recommendation the definitions set out in Directive 95/46/EC should apply. The following definitions should also apply:

(a) 'radio frequency identification (RFID)' means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it;

(b) 'RFID tag' or 'tag' means either a RFID device having the ability to produce a radio signal or a RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer;

(c) 'RFID reader or writer' or 'reader' means a fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags;

(d) 'RFID application' or 'application' means an application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked communication infrastructure;

(e) 'RFID application operator' or 'operator' means the natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using an RFID application;

(f) 'information security' means preservation of the confidentiality, integrity and availability of information;

(g) 'monitoring' means any activity carried out for the purpose of detecting, observing, copying or recording the location, movement, activities or state of an individual.

Privacy and data protection impact assessments

4. 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*.

5. Member States should ensure that operators, notwithstanding their other obligations pursuant to Directive 95/46/EC:

(a) conduct an assessment of the implications of the application implementation for the protection of personal data and privacy, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application;

(b) take appropriate technical and organisational measures to ensure the protection of personal data and privacy;

(c) designate a person or group of persons responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures to ensure the protection of personal data and privacy;

(d) make available the assessment to the competent authority at least six weeks before the deployment of the application;

(e) once the framework for privacy and data protection impact assessments as set out in point 4 is available, implement the above provisions in accordance with it.

Information security

6. Member States should support the Commission in identifying those applications that might raise information security threats with implications for the general public. For such applications, Member States should ensure that operators, together with national competent authorities and civil society organisations, develop new schemes, or apply existing schemes, such as certification or operator self-assessment, in order to demonstrate that an appropriate level of information security and protection of privacy is established in relation to the assessed risks.

Information and transparency on RFID use

7. Without prejudice to the obligations of data controllers, in accordance with Directives 95/46/EC and 2002/58/EC, Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy for each of their applications. The policy should at least include:

(a) the identity and address of the operators;

(b) the purpose of the application;

(c) what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored;

(d) a summary of the privacy and data protection impact assessment;

(e) the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks.

8. Member States should ensure that operators take steps to inform individuals of the presence of readers on the basis of a common European sign, developed by European standardisation organisations, with the support of concerned stakeholders. The sign should include the identity of the operator and a point of contact for individuals to obtain the information policy for the application.

RFID applications used in the retail trade

9. On the basis of a common European sign, developed by European standardisation organisations, with the support of concerned stakeholders, operators should inform individuals of the presence of tags that are placed on or embedded in products.

10. When conducting the privacy and data protection impact assessment as referred to in points 4 and 5, the operator of an application should specifically determine whether tags placed on or embedded in products sold to consumers through retailers who are not operators of that application represent a likely threat to privacy or the protection of personal data.

11. Retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy referred to in point 7, give their consent to keep tags operational. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer. Deactivation or removal of tags by the retailer should be done immediately and free of charge for the consumer. Consumers should be able to verify that the deactivation or removal is effective.

12. 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. Nevertheless, retailers should make available free of charge an easy means to, immediately or at a later stage, deactivate or remove these tags.

13. Deactivation or removal of tags should not entail any reduction or termination of the legal obligations of the retailer or manufacturer towards the consumer.

14. Points 11 and 12 should apply only to retailers that are operators.

Awareness raising actions

15. Members States, in collaboration with industry, the Commission and other stakeholders, should take appropriate measures to inform and raise awareness among public authorities and companies, in particular SMEs, of the potential benefits and risks associated with the use of RFID technology. Specific attention should be given to information security and privacy aspects.

16. Member States, in collaboration with industry, civil society associations, the Commission and other relevant stakeholders, should identify and provide examples of good practice in the implementation of RFID applications to inform and raise awareness among the general public. They should also take appropriate measures, such as large-scale pilot projects, to increase public awareness of RFID technology, its benefits, risks and implications of use, as a prerequisite for wider take-up of this technology.

Research and development

17. Member States should cooperate with industry, relevant civil society stakeholders and the Commission to stimulate and support the introduction of the 'security and privacy by design' principle at an early stage in the development of RFID applications.

Follow-up

18. Member States should take all necessary measures to bring this Recommendation to the attention of all stakeholders which are involved in the design and operation of RFID applications within the Community.

19. Member States should inform the Commission at the latest 24 months following the publication of this Recommendation in the *Official Journal of the European Union* of action taken in response to this Recommendation.

20. Within three years from the publication of this Recommendation in the *Official Journal of the European Union*, the Commission will provide a report on the implementation of this Recommendation, its effectiveness and its impact on operators and consumers, in particular as regards the measures recommended in points 9 to 14.

Addressees

21. This Recommendation is addressed to the Member States.

Done at Brussels, 12 May 2009.

For the Commission

Viviane REDING

Member of the Commission