

Orientation paper towards a
DRAFT COMMISSION RECOMMENDATION

of [...]

Commission Recommendation on the implementation of privacy, data protection and information security principles in applications supported by radio-frequency identification – "RFID Privacy, Data Protection and Security Recommendation"

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

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

Having regard to the opinion of the Economic and Social Committee,¹

After having consulted the European Data Protection Supervisor²,

Whereas:

- (1) Radio frequency identification (RFID) technology enables the processing of data, including personal data, over short distances by using radio frequencies, without physical contact or visible interaction between the reader and the tag, such that this interaction can happen without the individual concerned being aware of it.
- (2) RFID marks a new development in the Information Society where objects equipped with micro electronics that can process data automatically will increasingly become an integral part of every day life.
- (3) RFID technology has the potential to become a new motor of 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 increased efficiency, cost reductions and new business opportunities.
- (4) RFID has entered the public space, and hence affects life of individuals, with diverse applications such as those for the retail sector, the leisure sector, the working environment, public transport, highway toll management, luggage management, and travel documents.
- (5) Because of its potential to be both omnipresent and practically invisible, particular attention to transparency, privacy and data protection, and information security related issues is required in the deployment of these devices. In this regard, privacy and

¹ TEN/293 Radio Frequency Identification (RFID), 11 July 2007.

² OJ

information security features should be built into the RFID applications before their widespread use ("security and privacy-by-design").

- (6) Research and Development on low cost RFID privacy and information security technologies and applications is essential at Community level to promote a wider take up of these technologies under acceptable conditions.
- (7) The Commission Communication of 15 March 2007 on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework (COM(2007)96 final) announced clarification and guidance on RFID data protection and privacy aspects of RFID applications through one or more Commission Recommendations before the end of 2007.
- (8) The Commission Decision 2007/467/EC of 28 June 2007³ set up the Expert Group on Radio Frequency Identification to provide advice to the Commission on the content of this Recommendation.
- (9) The Council Resolution of 22 March 2007 on a strategy for a secure information society in Europe has invited Member States to strengthen the contribution to security related R&D and to improve the usability and dissemination of the consequential results.
- (10) RFID will only be able to deliver its numerous economic and societal benefits if effective measures are in place to safeguard personal data protection, information security, privacy and the associated ethical principles that are central to the debate on the public acceptance of RFID.
- (11) This Recommendation respects the fundamental rights and observes the principles reflected in the Charter of Fundamental Rights of the European Union as proclaimed on 14 December 2007, in particular Article 7 "Respect for privacy and family life" and Article 8 "Protection of personal data" thereof.
- (12) The rights and obligations concerning the protection of personal data and the free movement of such data as provided for in Directive 95/46/EC of the European Parliament and of the Council of 24 October 95 on the protection of individuals with regard to the processing of personal data and on the free movement of such data⁴, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on privacy and electronic communications⁵, and 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 conformity⁶, are fully applicable to the use of RFID applications that process personal data.
- (13) RFID applications hold the potential to process data relating to an identified or identifiable natural person, a natural person being identified directly or indirectly. RFID applications can process personal data stored on the tag such as a person's name,

³ OJ L 176, 6.7.2007, p. 25–30.

⁴ OJ L 281, 23.11.95, p.31–50.

⁵ OJ L 201, 31.7.2002, p. 37–47.

⁶ OJ L 91, 7.4.1999, p. 10–28.

birthday or address or biometric data or data connecting a specific RFID item number to personal data that is stored elsewhere in the system. RFID has also the potential to monitor an individual through his/her possession of one or more items that contain a RFID item number.

- (14) The RFID application operator should take all reasonable steps to ensure that data is not related to an identified or identifiable natural person through any reasonable means likely to be used by either the RFID application operator or any other person.
- (15) The Commission Communication of 2 May 2007 on Promoting Data Protection by Privacy Enhancing Technologies (PETs) (COM(2007)228 final) sets out clear actions to achieve the goal of minimising the processing of personal data and using anonymous or pseudonymous data where possible by supporting the development of PETs and their use by data controllers and consumers.
- (16) An assessment of the information security risks and privacy impacts prior to the implementation of a RFID application will provide necessary information for appropriate protective measures that need to be monitored and reviewed throughout the lifetime of the RFID application.
- (17) Those affected by RFID use should have recourse to legal redress, without prejudice to any administrative remedy for which provision may be made before the competent authority, to claim compensation both as required by law and with regard to any improper use of RFID that has affected them.
- (18) The existence and use of standards and best practices can help to manage information security and privacy measures throughout the whole RFID-enabled business process.
- (19) 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, their implications with medical legislation and, therefore require specific attention.
- (20) Diversity, openness, interoperability, usability and competition have been acknowledged as key drivers for information security in the Commission Communication: a strategy for a Secure Information Society - "Dialogue, partnership and empowerment" (COM(2006)251 final), and these principles need therefore to be applied to RFID applications.
- (21) Society as a whole needs to be aware of the obligations and rights that are applicable in relation to the use of RFID and the parties that deploy the technology, such as equipment manufacturers, commercial operators, public entities and Member States administrations, therefore have a responsibility to provide the public with information on RFID use.
- (22) Raising awareness with the public and small and medium enterprises (SME) in particular will help allow RFID to fulfil its economic promise by informing them on the features and capabilities RFID technology, thus mitigating the risks of this technology being used to the detriment of the public interest and enhancing its acceptability.

- (23) Member States and stakeholders should, especially in this initial phase of RFID applications implementation, dedicate further efforts to assuring that RFID applications are monitored and the rights and freedoms of individuals are respected.
- (24) The purpose of this Recommendation is to provide guidance by identifying principles in relation to RFID use that would seek to ensure maximizing benefits of RFID use without compromising the right to integrity, privacy and data protection of the individual in a democratic society.
- (25) EDPS Opinion of December 2007...

HEREBY RECOMMENDS THAT:

Article 1

Scope

1. This Recommendation provides guidance to Member States and stakeholders on the design and operation of RFID applications in a lawful, ethically admissible and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data and appropriate information security.
2. This Recommendation concerns measures to be taken with respect to the implementation of RFID applications, which will ensure that national legislation implementing Directives 95/46/EC, 99/5/EC and 2002/58/EC is respected when such applications are deployed. This Recommendation is without prejudice to the legal obligations resulting from the national legislation implementing Community Law.
3. This Recommendation shall not apply to activities which fall outside of the scope of the Treaty establishing the European Community, such as those referred to in titles V and VI of the Treaty of the European Union, and in any case to activities concerning public security, defence, state security and the activities of the state in the areas of criminal law.

Article 2

Definitions

For the purpose of the Recommendation the definitions set out in Directive 95/46/EC shall apply. The following definitions shall 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 type of device) and modulates a carrier signal received from a reader.

(c)'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' means a system to process data through the use of RFID tags and/or readers, a back-end system and/or a networked communication infrastructure.

(e)'RFID application operator' means the natural or legal person who develops, implements, uses or maintains a RFID application.

(f)'Information security' means the preservation of 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, image, text, voice, sound or state of an individual.

(h)'Deactivation' of a tag means the process that causes the cessation of any functionality of the RFID tag. The deactivation can be *permanent*, so that the tag no longer responds to any command, or can be *temporary*, so that the tag only responds to specific commands that make the tag partially or entirely functional again.

(i)'Public place' means any area, including non-stationary means of public transport such as buses, planes, railways or ships, which can be accessed at all times or at certain times by everybody.

Article 3

Privacy and Data Protection measures

1. Before a RFID application is implemented, the RFID application operators should conduct, individually or jointly within a common value chain, a privacy impact assessment to determine what implications its implementation could raise for privacy and the protection of personal data, and whether the application could be used to monitor an individual.

2. The level of detail of the assessment should be proportionate to the risks associated with the particular RFID application. The assessment should comply with good practice frameworks to be established in a transparent way in partnership with all relevant stakeholders, and in consultation of the relevant supervisory data protection authorities.

3. Where it cannot be excluded that data processed in RFID applications can be related to an identifiable natural person by an RFID application operator or a third party, Member States should ensure that RFID application operators and providers of components of such applications take appropriate technical and organisational measures to mitigate the ensuing privacy and data protection risks.

4. RFID application operators should designate a person responsible for the conduct, review, and follow-up measures as described above.

5. The RFID application operator should align the privacy impact assessment with the overall information security risk management set out in Article 6 here after.

6. The RFID application operator should make the privacy impact assessment, or an adequate and comprehensible summary of it, publicly available through appropriate means, no later than on the date of deployment of the application.

Article 4

Codes of Conduct

1. Member States should encourage trade or professional associations or organisations involved in the RFID value chain to provide detailed guidance on practical implementation of RFID technology by drawing up specific codes of conduct on RFID use. Where appropriate, this work should be undertaken in collaboration with the concerned civil society organisations, such as consumer organisations or trade unions, and/or the competent authorities concerned. Codes of conduct should contain specific measures designed to ensure that signatories adhere to their principles. They should be widely disseminated with a view to informing affected individuals.

2. With regard to data protection aspects, Member States should encourage drawing up of codes of conduct intended to contribute to proper implementation of the national provisions adopted pursuant to the Directive 95/46/EC, taking account of the specific features of the various sectors.

3. In conformity with Directive 95/46/EC, national codes of conduct should be submitted to the relevant national supervisory data protection authorities for endorsement, and Community codes of conduct should be submitted to the Article 29 Working Party for endorsement at Community level.

Article 5

Information on RFID use

1. Where RFID applications are implemented in public places, RFID application operators should make publicly available a written comprehensible policy governing the use of their RFID application. Without prejudice to the obligations of data controllers, in accordance with Directives 95/46/EC and 2002/58/EC, the policy should state:

- (a) the identity and address of the RFID application operator,
- (b) the purpose of the RFID application,
- (c) what data is to be processed by the RFID application, in particular if the location of tags will be monitored,
- (d) which link, if any, is made with personal data,
- (e) what is the data storage policy followed by the operator,
- (f) if the data can be accessed or received by third parties.

The policy should be concise and generally understandable by individuals.

2. Where RFID applications are implemented in public places, RFID application operators should inform individuals on the use of RFID by providing at least a clear sign, accessible by all, that signifies the presence of RFID readers. Information should include, where appropriate, that RFID tags and readers may broadcast information without an individual engaging in any active action, a reference to the policy governing the use of the RFID application and a point of contact for individuals to obtain additional information.

Article 6

Information security risk management

1. Member States should encourage RFID application operators to establish information security management according to state-of-the-art techniques, based on effective risk management in order to ensure appropriate technical and organisational measures related to the assessed risks. The security threats, and the corresponding security measures, should be understood as covering all the components and interfaces of the RFID application.

2. Member States should provide guidance to identify those RFID applications that might be exposed to information security threats with implications for the general public. Member States should also stimulate RFID application operators that provide these applications to develop application-specific guidelines, in partnership with all concerned stakeholders. Public and private sector organisations should strive to ensure that their members comply with these guidelines. The dissemination of Best Available Techniques for these applications at European level should be encouraged with a view to achieving a coherent internal market approach towards information security.

3. Member States should encourage the RFID application operators, together with national competent authorities and civil society organisations, to develop new, or apply existing, schemes, such as certification or operator self-assessment declaration, in order to demonstrate that an appropriate level of privacy and information security is established in relation to the assessed risks, related to RFID applications.

Article 7

RFID use in retail

1. RFID application operators acting at any level of the value chain should ensure that they provide sufficient information and means to operators down the chain so that the provisions of this recommendation can be followed.

2. RFID application operators, where appropriate in cooperation with retailers, should adopt a harmonised sign to indicate the presence of tags within retail products and ensure that consumers are informed:

- about the presence of a RFID tag in a retail product;
- whether this tag has a specified, explicit and legitimate purpose after the sale;
- about the likely reasonable privacy risks relating to the presence of the tag and of the measures consumers can take to mitigate these risks.

3. (a) Where a RFID application processes personal data or the privacy impact assessment (undertaken in accordance with Art 3.1) shows significant likelihood of personal data being generated from the use of the application, the retailer has to follow the criteria to make the processing legitimate as laid down in directive 95/46 and to deactivate the RFID tag at the point of sale unless the consumer chooses to keep the tag operational.

(b) Where a RFID application does not involve processing of personal data and where the privacy impact assessment has shown negligible risk of personal data being generated through the application, the retailer must provide an easily accessible facility to deactivate or remove the tag.

4. Deactivation or removal of tags should not entail any reduction or termination of the legal obligations of the retailer or manufacturer towards 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 action is effective.

5. Within three years after the entry into force of this recommendation, the European Commission will review these provisions in order to assess the effectiveness and efficiency of systems to remove or deactivate tags, with a view to providing automatic deactivation at the point of sale on all items except where the consumer has specifically opted-in to the RFID application.

Article 8

Awareness raising actions

1. Member States, in collaboration with industry and other stakeholders should take appropriate measures to inform and raise awareness among companies, in particular SMEs, on the potential benefits associated to the use of RFID technology. Specific attention should be placed on information security and privacy aspects.

2. Member States, in collaboration with industry, consumer associations and other relevant stakeholders, should identify and provide examples of good practice in RFID application implementations. They should also take appropriate measures, such as large-scale pilots, to increase public awareness of RFID technology, its benefits and implications of use, as a prerequisite for wider take-up of this technology.

Article 9

Research and Development

Member States should cooperate with industry and the Commission to stimulate and support the introduction of the 'security and privacy by design' principle at an early stage of the development of RFID applications, in particular through the development of high-performance and low-cost solutions.

Article 10

Follow-up

1. Member States should inform the Commission 18 months from the publication of this Recommendation in the Official Journal of the European Union of action taken in response to this Recommendation.

2. Within three years from the entry into force of this Recommendation, the Commission will provide a report on the implementation of this Recommendation and its impact on economic operators and consumers, in particular as regards the measures recommended in Article 7. Where appropriate, the Commission shall amend this Recommendation or submit any other proposal it may deem necessary, including binding measures, in order to better achieve the goals of this Recommendation.

Article 11

Entry into force

This Recommendation shall enter into force on the day of its publication in the Official Journal of the European Union.

Article 12

Addressees

This Recommendation is addressed to the Member States and to all stakeholders which are involved in the design and operation of RFID applications within the Community.

Done at Brussels, [...]

For the Commission

[...]

Member of the Commission