INTRODUCTION TO THE PUBLIC CONSULTATION ON THE RFID PRIVACY, DATA PROTECTION AND SECURITY RECOMMENDATION

1. BACKGROUND

Following a first public consultation on Radio Frequency Identification (RFID) held in 2006[1], the Commission has, through its Communication of 15th March 2007[2], committed itself to address some of the issues expressed by stakeholders regarding the risks to privacy, data protection and security by adopting a Recommendation on this matter.

Given the importance of this subject, the Commission has decided to put up for public consultation all the articles that are currently being considered in its draft Recommendation.

2. PREPARATION OF THIS DRAFT RECOMMENDATION

Three conferences on RFID in Brussels[3], Berlin[4] and Lisbon[5] have directly contributed to the debate and the thought process behind the preparation of this Recommendation.

The Commission has created an Expert Group[6], *the RFID Expert Group*, to, inter alia, provide advice to the Commission on the content of such Recommendation.

Finally, a number of other contributions have been considered while preparing this work. Some examples include the European Economic and Social Committee (EESC)[7], the Article 29 Data Protection Working Party[8][9], the European Data Protection Supervisor[10] and the OECD[11].

CALENDAR AND NEXT STEPS

The Public Consultation will be open for a period of eight weeks and will finish on 25th April 2008. A translation of this consultation in French and German is also available on this site.

The Recommendation is tentatively scheduled to be adopted before the summer of 2008.

---

1 http://ec.europa.eu/information_society/policy/rfid/doc/rfidswp_en.pdf
2 COM/2007/96 - Radio Frequency Identification (RFID) in Europe: steps towards a policy framework.
3 EU RFID Forum, 13-14 March 2007.
4 http://www.nextgenerationmedia.de/Nextgenerationmedia/Navigation/en/rfid-conference.html
5 http://www.rfid-outlook.pt/
6 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:01:EN:HTML and http://ec.europa.eu/information_society/policy/rfid/doc/reg.pdf
7 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_256/c_25620071027en00660072.pdf
8 Opinion 4/2007 of 20 June 2007 - http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf
9 See Opinion 105 and 136 (conclusions): http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm
10 See Opinion of 20th December 2007: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/26
11 http://www.oecd.org/dataoecd/59/12/36069207.pdf

ANSWERING PROCESS

Each question corresponds to one article of the draft Recommendation. It is made of a short introduction followed by the envisaged text. The Commission does not foresee any additional article, but this could change depending on the inputs gathered as part of this consultation. The final question is a white box for any additional comment that you might have that is not directly linked to a given article. All questions are optional, meaning that you can leave blank any question on which you do not want to comment.

Please respect the following rules when replying to the questions:

– Answer each question where indicated and limit yourself to the space made available (i.e. don't use the space provided for question 4 to finish a reply to question 3).

– Your answers need to be self-explanatory, without requiring the reading of external documents to be understood. References to outside documents are welcomed but, for practical reasons, we cannot guarantee that all will be read.

– Only the 20 lines of each answer (30 for the last question) will be saved by the system. Longer answers will be truncated and won't therefore be usable.

– Answers that fall outside of the scope of the question will not be considered.

Unless otherwise requested by the respondent, all contributions will be made public by the Commission after the end of the consultation on its web site.

You will find here the Privacy Statement.

RESPONDENT DETAILS

Last Name (optional)

First Name (optional)

Gender

Male Female

E-mail address (compulsory)

What type of stakeholder are you? (compulsory)

Interested citizen

Consumer Advocacy Group

Labour organisation

Governmental organisation

RFID using industry

RFID consulting industry

RFID (systems) industry

NGO

International Organisation

Academic

Telecommunications

Other

Please indicate your age group (optional)

Under 18

18-24

25-44

45-64

65+

Your organisation's country of establishment (indicate your country of residence if answering as an individual person) (compulsory)

Algeria, Argentina, Austria, Australia, Belgium, Bolivia, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany Greece, Hong Kong, Hungary, Iceland, India, Ireland, Israel, Italy, Japan, South Korea, Liechtenstein, Lithuania, Latvia, Luxembourg, Macedonia, Malta, Mexico, Morocco, Netherlands, New Zealand, Norway, Other, Poland, Portugal, Romania, Russia, Singapore, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, Tunisia, Turkey, Ukraine, United Kingdom, United States

Your organisation's geographic area of activity (please indicate your geographic area of activity if answering as an individual person) (optional)

Local

Regional

National

European Commission International

INDIVIDUAL QUESTIONS INTRODUCTION

Question 1 – Scope	
The Recommendation focuses on the privacy, data protection and information security aspects of RFID technology deployment and is intended to provide guidance in this respect to EU Member States and to stakeholders. It is *not* intended to cover other important policy issues that were addressed in the Communication "*RFID in Europe: steps towards a policy framework"*, namely the governance of resources in the Internet of Things, technology development and innovation, radio spectrum, standards, environment and health (para 1). The Recommendation shall provide guidance on the practical implementation of the principles defined in the Data Protection Directive 95/46/EC, the Directive on radio equipment and telecommunications terminal equipment 99/5/EC and the Directive on Privacy and electronic communications 2002/58/EC whose text can be found here[12] (para 2). The Recommendation does not address the domains of Common Foreign and Security policy and of police and judicial cooperation in criminal matters. The proposed article on the scope reads as follows (para 3):	*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.

[12] http://eur-lex.europa.eu/RECH_naturel.do

Question 2 – Definitions	
The Recommendation uses the definitions from the Data Protection Directive. In addition, RFID specific terms are defined, taking into account existing international technical standards. The proposed article on the definitions reads as follows:	*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.

Question 3 – Privacy measures	
This article provides guidance on implementing RFID applications in such a way that compliance with data protection and privacy legislation can be ensured practically. As a first step, a systematic analysis of the privacy risks (Privacy Impact Assessment PIA) is recommended, before any application is implemented (para 1 & 2). The results should be made publicly available in appropriate form (para 6). The use of PIAs is an established methodology and some examples of uses can be found here[13]. The privacy impact analysis will also provide input to the design process of the RFID application, such that risks can be minimised. The implementation of appropriate measures to mitigate risks is recommended (para 3). It is important that clear organisational responsibility for these measures is allocated (para 4). The privacy impact assessment should provide input and be coordinated with the general information security risk management as recommended in Article 6 of the Recommendation (para 5). The proposed article on privacy measures reads as follows:	*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.

[13] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

	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.

Question 4 – Codes of conduct	
Acknowledging the diversity of RFID applications and the likely widespread use that organisations will make of them, this article encourages the development of sector and/or application specific codes of conduct with binding measures for its signatories (para 1). Similarly, the article 27 of the Data Protection Directive foresees the development of codes of conduct to cover data protection aspects (para 2). The provisions of this article recommend that, when such aspects are addressed by the codes of conduct, they are submitted for endorsement to the relevant Data Protection Authorities (para 3). The proposed article on codes of conduct reads as follows:	*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.

Question 5 – Information on RFID use	
RFID applications can technically operate without any visible or otherwise perceivable action, so that nobody can directly observe any transactions. The provisions of this article aim at setting the minimum information to be provided by RFID operators to individuals, in the form of written policies (para 1) and signs (para 2) informing on the presence of RFID readers in public places. In addition, when Codes of Conduct are enacted according to Article 4 of the Recommendation, these may require, for example, providing more detailed and comprehensive information to the consumer. It should be noted that article 7 (RFID use in retail) foresees additional information requirements in the case of the retail sector. The proposed article on Information on RFID use reads as follows:	*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.

Question 6 – Information security risk management	
RFID applications, as any information technology, need to operate in a secure manner. In line with the Commission Communication: "*a strategy for a Secure Information Society - Dialogue, partnership and empowerment"* (COM(2006)251 final), this article details measures to be taken with respect to the information security of RFID applications. The proposed article on the information security risk management reads as follows:	*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.

Question 7 – RFID use in retail applications	
The recommendations concerning privacy measures, self regulation (codes of conduct), information on RFID use, and information security risk management are applicable to *all* RFID applications and to *all* economic and social sectors. However, it is believed that the *retail sector* requires additional guidance because of the specific characteristics derived from the potentially large dissemination of consumer products carrying RFID tags. The Article recommends information to consumers which can be presented in the form of a logo as well as any piece of information allowing consumers to make an informed choice (para 2). In accordance with Directive 95/46, the article recommends that tags that contain personal data should be subject to the "opt-in" principle at the point-of-sale, that is that tags are deactivated by default unless the consumer wants to keep them active (para 3a). When no personal data are involved, the article recommends that retailers need to make available the means to deactivate or remove the tags if consumers request it. (para 3b). The European Commission will analyse the effectiveness and the efficiency of the tag removal and deactivation systems. The long term goal is that, through appropriate Research and Development, tags can be easily deactivated or removed, unless the consumer opts to keep tag functioning (Para 5). The proposed article on the RFID use in retail applications reads as follows:	*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.

Question 8 – Awareness-raising actions	
As witnessed with the public consultation of 2006, and regularly confirmed by all stakeholders, the true benefits and risks born by RFID technologies are widely unknown by both the general public and even by many enterprises, in particular SMEs. The following measures are aimed at raising awareness on the RFID technology in order to support its development while at the same time addressing the concerns of all the users. The proposed article on awareness-raising actions reads as follows:	*Article 8* Awareness raising actions 1. Members 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.

Question 9 – Research and development	
This article recommends putting particular focus of research and development efforts on strong security and privacy features in affordable RFID components and systems. The proposed article on research and development reads as follows:	*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.

Question 10 – Follow-up	
RFID technologies, and their usage, evolve very quickly. Acknowledging that not all implications of yet-to-come applications are foreseeable, the Commission is committed to continue its work in this area beyond the adoption of this Recommendation and does so by proposing the following provisions:	*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 adoption 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.

Question 11 – Addressees	
Acknowledging that the successful large-scale deployment of RFID technology does not only lie in the hands of public authorities, but as well other stakeholders, the Commission proposes to address the Recommendation to both with the following provision.	*Article 11* 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.

Question 12 – Additional comments	
Participants to this consultation who are interested in submitting additional comments that are not directly linked to a given article but rather cover the entire Recommendation or that fall outside of the suggested articles are invited to do so here.	