I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96

(2008/C 101/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to 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,

Having regard to 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,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 15 March 2007, the Commission adopted a Communication on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework ([1]) (further: 'the Communication'). Under Article 41 of Regulation (EC) No 45/2001, the EDPS is responsible for advising Community institutions and bodies on all matters concerning the processing of personal data. In accordance with this Article, the EDPS presents this opinion.

2. This opinion must be seen as a reaction of the EDPS on the Communication, as well as on other actions in the area of RFID that have taken place since the adoption of the Communication. These other relevant actions that have been taken into account in this opinion include:

— the Commission Decision of 28 June 2007 setting up the Expert Group on Radio Frequency Identification ([2]), a direct consequence of the Communication. This group is also known as the RFID-Stakeholders Group. In accordance with Article 4(4)(b) of the decision, the EDPS participates to the activities of the group as an observer,

— the Council Resolution of 22 March 2007 on a strategy for a secure Information society in Europe ([3]),

— the Project 'RFID and identity management' initiated by the European Parliament ([4]),

([1]) COM (2007) 96 final.
([2]) Decision No 467/2007/EC (OJ L 176, 6.7.2007, p. 25).
([3]) OJ C 68, 24.3.2007, p. 1.
([4]) Project 'RFID and identity management — Case studies from the frontline of the development towards ambient intelligence', commissioned by the Scientific Technology Option Assessment service (STOA) of the European Parliament and carried out by the ETAG (European Technology Assessment Group) http://www.europarl.europa.eu/stoa/default_en.htm

— the adoption by the Article 29 Data Protection Working Party in June 2007 of Opinion No 4/2007 on the concept of personal data ([1]),

— the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive ([2]), and the opinion of the EDPS on this communication of 25 July 2007 ([3]),

— the adoption by the Commission of a proposal for a Directive amending (*inter alia*) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ([4]).

3. The EDPS welcomes the Commission's Communication on RFID as it tackles the main issues arising in the context of the deployment of RFID technology without neglecting the determinant ones related to privacy and data protection. This communication has benefited from consistent and rigorous preparatory works. Indeed, five thematic workshops as well as an online public consultation ([5]) commissioned by the Commission have preceded this communication.

4. The EDPS agrees with the view that RFID systems could play a key role in the development of the Information Society usually referred to as the 'Internet of things' and he also fully shares the concerns mentioned in paragraph 3.2 of the Communication that RFID systems may threaten individual's privacy and data protection rights. Indeed, in his Annual Report 2005, the EDPS identified RFID together with biometrics, ambient intelligence environments and Identity Management Systems, as technological developments that are expected to have a major impact on data protection.

5. According to the EDPS, the domestication of RFID technologies and their wide acceptance will not only be reached by their attractive convenience or the new services they offer, but will also be facilitated by the benefits of well-tailored and consistent data protection safeguards.

6. In short: the EDPS qualifies RFID as a fundamentally new technological development, rightly referred to in the Commission's Communication as the gateway to a new phase of development of the Information Society.

7. This development raises important questions in different areas, one of which is the area of data protection and privacy. This opinion of the EDPS is limited to this area.

II. FOCUS OF THE OPINION

8. This opinion is in particular focused on the possible consequences of these developments for data protection and privacy. These consequences are at the moment uncertain, also due to the fact that the development of RFID-systems and their domestication are in full progress and that it is in no way clear where these developments will end.

9. In this perspective, the EDPS takes the following approach:

— in the first place, it is needed to clarify the practical consequences of the deployment of the RFID-systems for data protection and privacy,

— in the second place, it is needed to specify these consequences, in the context of the existing legal framework for data protection and privacy,

— in the third place, the EDPS addresses the question whether these consequences require more specific rules to tackle data protection issues raised by the use of RFID-technologies. This issue was already brought forward by the EDPS in his Opinion on the Communication on the Data Protection Directive and will be elaborated further in the present opinion.

10. By taking this approach, the EDPS aims to promote that the development of RFID-systems and their domestication will take account of justified data protection and privacy concerns.

III. CLARIFYING THE CONSEQUENCES

RFID systems and tags

11. Despite the fact that — as said — the developments are in full progress and the outcome is uncertain, it is very well possible to describe the main characteristics of these developments with a view to their consequences for data protection.

([1]) Document WP 136, published on the website of the Working Party.
([2]) Commission Communication of the European Parliament and of the Council of 7 March 2007 on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final.
([3]) OJ C 255, 27.10.2007, p. 1. Further: 'Opinion on the Communication on the Data Protection Directive'.
([4]) Proposal of 13 November 2007 for a Directive of the European Parliament and the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, 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, Regulation (EC) No 2006/2004 on consumer protection cooperation, COM(2007) 698 final. Directive 2002/58/EC will be referred to as 'ePrivacy Directive'.
([5]) http://www.rfidconsultation.eu/

12. In assessing the potential data protection and privacy aspects of RFID technology, it is highly relevant to not only consider RFID tags alone, but the overall RFID infrastructure: the tag, the reader, the network, the reference database and the database where the data produced by the association tag/reader are stored. As is briefly underlined in the introduction of the Communication, RFIDs are not just 'electronic tags' and therefore data protection issues will not be exclusively limited to tags, but extend to all parts of the overall RFID infrastructure. Indeed, each of these elements has a role in contributing to the implementation of the European data protection legal framework when it is required. They will be fuelled by the main trends within the developing Information Society, such as an almost unlimited bandwidth, ubiquitous network connections and an endless storage capacity.

Impact of RFID systems and tags

13. Notwithstanding the need for a wider approach as emphasised in the preceding paragraph, various reasons justify focussing first on the use of RFID in item level tagging in consumer products like the retail sector. The obvious one is its foreseen increased use, which seems to be moving towards its widespread application. As opposed to other RFID applications with narrow or limited use, item level tagging has the potential to become a mass market application. Already now many consumer products are equipped with a RFID tag. Linked to this is the fact that such use will affect a huge number of individuals whose personal data are likely to be processed each time they acquire a product in which a RFID tag is embedded.

14. Specific attention should be given to the consequences of RFID tagging for the owners of items. RFID systems might stretch out the relationship between an item and its owner. Once this relationship is stretched out, the owner can be scanned and classified as 'low budget' or 'attractive target' for future transactions; excessive one-to-one attribution ([1]) might be conducive to automatic 'punishment' of certain behaviour (recycling obligation, waste, etc.). Individuals should not be subject to the process of adverse automated decisions. Catalysed by this RFID ability, the risk increases that the Information Society moves closer to a situation where automated decisions will be taken and where technology will be abused in order to regulate the human behaviour.

15. The data stored in or produced by an RFID tag, can be personal data as defined in Article 2 of the Data Protection Directive. For example, smartcards used for travel may contain identification information as well as information about the holder's recent journeys. If an unscrupulous individual wanted to track individuals, it would be sufficient to strategically place readers which would provide information about the movements of card holders, thus violating their privacy and personal information.

16. Similar privacy threats could happen even if the information stored in the RFID tag would not include names of individuals. RFID tags contain unique IDs attached to consumer products: if each tag has a unique ID, such identification can be used for surveillance purposes. For example, if someone wears a watch that carries an RFID tag containing an ID number, this could also serve as a unique identifier for the wearer of the watch, even if his identity is not known. Depending on the way the information is used — and put in relation with the watch itself or the individual — the Directive could apply or not. It would apply, for instance, if information is generated about the whereabouts of individuals that is likely to be used to monitor their behaviour, or for example for price differentiation, denying access, or unwanted exposure to publicity.

17. In this context, it is necessary to ensure that RFID applications are deployed with the necessary technological measures to minimise the risk of unwilling disclosure of information. Such measures may include the requirement to design the RFID infrastructure, particularly RFID tags, in a way that prevents such an outcome. For example, RFID tags can be deployed with a 'kill command' allowing their deactivation. This option will be further discussed in Chapter IV of this Opinion.

18. By offering the possibility to track products after the point of sale, RFID systems introduce new issues in the privacy debate. Indeed, two elements will have to be taken into account in the analysis of their impact: how personal the item is considered to be, and the mobility of the item ([2]).

19. The life cycle of an object might also complement the required risk analysis and contribute to the quantitative assessment of the potential threats regarding privacy. Considering the fact that a tag may not be deactivated, an end-user product with a long life cycle will be able to gather more related data from the owner of the product and build a more accurate profile. On the other hand, a short life cycle of an item like a can of soda from its production until its recycling step might present fewer risks and could request therefore lighter measures than a product with a much longer life cycle.

([1]) Dr Sarah Spiekermann, Director Berlin Research Centre on Internet Economics, workshop on RFID and ubiquitous computing organized by the Trans Atlantic Consumer Dialogue, 13 March 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman and Norman G. Einspruch, Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology, Volume 9, No 2/2007.

Privacy and data protection issues in RFID system deployment

20. In order to better understand the consequences of RFID-systems for privacy and data protection, five basic privacy and security issues can be distinguished.

21. The first issue is identification of the data subject. More than sixty years ago, the purpose of the RFID tag was to 'Identify the Friend or Foe' coming. Today RFID systems can not only identify general elements of an object but can also ultimately lead to the identification of an individual and need therefore to do it in a data protection friendly way.

22. The second issue is identification of the controller(s). In the case of RFID systems, the identification of the controller as defined in Article 2(d) of the Data Protection Directive, might be more difficult and therefore needs closer examination. However, identifying the controller remains a critical step in establishing the responsibilities of each of the relevant actors who will have to comply with the data protection legal framework. During the lifecycle of the tag, the controller who processes the data could change several times based on the additional services which can be provided in relation to the tagged object.

23. The third issue is the decreased meaning of the traditional distinction between the personal and the public sphere. Although the distinction between private and public spaces has also in the past not always been clear-cut, most people are aware of the boundaries between them (and of the grey zones) and take informed or intuitive decisions on how to act accordingly. According to Hall ([1]), personal space is usually translated into physical distance from others. Privacy management can also be considered as a dynamic boundary regulation process ([2]). It is therefore not surprising that the wireless nature of the tag communication as well as its outside of line-of-sight reading capability, raise privacy concerns by blurring these traditional borders and their management. Indeed, there are fears that the individual may lose some or all control on distance management that he/she has enjoyed until now. Accordingly, the reading range of the first implementations of RFID systems has been targeted equally by their promoters and detractors.

24. The fourth issue has to deal with the size and the physical properties of RFID-tags. Because the tag needs to be basically small and cheap, the security measures which could be deployed on this part of the RFID system will be by definition limited. However, the wireless aspect of the communication also adds a layer of risks compared to a wired communication and therefore additional security requirements are needed.

25. The fifth issue is the lack of transparency of the processing. RFID systems may lead to unnoticed gathering and processing of information capable of being used for profiling an individual. This consequence may very well be illustrated by comparing RFID-systems to the mobile phone, a comparison that is made more often. On the one hand, the mobile phone benefited of a very high level of technology acceptance independently of potentially intrusive privacy risks. One could conclude that RFID will be accepted in the same manner. On the other hand, it has to be underlined that a mobile phone is a visible object which is still under the control of the end user as it can be switched off. This is not the case with RFID.

26. Although unnoticed gathering and processing of information as mentioned above may be legitimate, it is also possible and under various circumstances even quite likely that illegitimate collection and processing of such data occurs.

27. The clarifications of this chapter justify the following conclusion. The wide use of RFID-technology is fundamentally new and may have a fundamental impact on our society and on the protection of fundamental rights in our society, such as privacy and data protection. RFID may bring about a qualitative change.

IV. SPECIFYING THE CONSEQUENCES

Introduction

28. This chapter will mainly focus on the impact of RFID on the protection of fundamental rights in our society, such as privacy and data protection. This will be specified in two steps, the first step being a short description of the way in which these fundamental rights are protected under the present legal framework. As a second step, the EDPS will elaborate on the possibilities to fully use the present legal framework. This aspiration has been introduced in the Opinion on the Communication on the Data Protection Directive as 'the full implementation of the present provisions of the Directive'.

29. The point of departure is as follows: new technological developments such as RFID systems, have a clear impact on the requirements for an effective legal framework for data protection. Also, the need for effective protection of the personal data of an individual can impose limitations on the use of these new technologies. Interaction is thus two-sided: the technology influences the legislation and the legislation influences the technology ([3]).

([1]) Hall, E.T., 1966. The Hidden Dimension (1st ed.), Garden City, N.Y.: Doubleday.

([2]) Altman, I. 1975, The Environment and Social Behaviour, Brooks/Cole Monterrey.

([3]) See the EDPS comments of March 2006 on the Commission communication on the interoperability of European databases, published on the EDPS-website.

Protection of fundamental rights

30. The protection of the fundamental rights to privacy and data protection within the European Union is in the first place guaranteed by a legislative framework, which is needed since we deal with rights that are recognised in Article 8 of the European Convention of Human Rights and Fundamental Freedoms and in Article 7 and Article 8 of the Charter of Fundamental Rights of the Union. The relevant legislative framework for data protection and RFID basically consists of the Data Protection Directive 95/46/EC and the ePrivacy Directive 2002/58/EC ([1]).

31. The general legislative framework for data protection as laid down in Directive 95/46/EC applies to RFID, as far as data processed by RFID systems fall within the definition of personal data. Whereas in certain cases RFID applications clearly process personal data and undoubtedly fall within the scope of the Data Protection Directive, there are also applications where the applicability of the Data Protection Directive may not be so obvious. The Article 29 Data Protection Working Party's Opinion No 4/2007 on the concept of personal data aims to contribute to a clearer and commonly recognised understanding of the concept of personal data and, by doing so, mitigate this uncertainty ([2]).

32. As far as the ePrivacy Directive is concerned, the situation is as follows. Until now, it is not clear whether this Directive applies to RFID applications. For this reason, the Commission Proposal of 13 November 2007 for amendment of the Directive contains a provision aiming to specify that the Directive indeed applies to certain RFID applications. However, other RFID-applications might not be covered because of the limitation of this Directive to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

33. The protection of personal data can be complemented by a range of self-regulatory instruments (non-legislative framework). The use of those instruments is actively promoted in both directives, in particular in Article 27 of the Data Protection Directive that provides that the Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the Directive. Moreover, self-regulatory instruments could efficiently contribute to the implementation of the security measures requested by Article 17 of the Data Protection Directive and Article 14 of the ePrivacy Directive.

([1]) Point 59 of this Opinion will discuss the relevance of a third directive, namely 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 (OJ L 91, 7.4.1999, p. 10).

([2]) See *inter alia* p. 10 of the Opinion, quoted in footnote 5.

Full implementation of the existing framework

34. The Opinion on the Communication on the Data Protection Directive lists a number of tools available for a better implementation of the Directive. Most of the non binding tools of that opinion are relevant to RFID, such as interpretative communications or other communications, promotion of best practices, the use of privacy seals and third-party privacy audits. The possibility of adopting specific rules for RFID will be discussed in Chapter V. But improvements are possible also within the current framework.

Self-regulatory instruments

35. The EDPS agrees with the Commission that in a first phase it is appropriate to leave room for self-regulation, enabling stakeholders to create quickly a legally compliant environment and thus contributing to create a more secure legal environment.

36. The Commission, in consultation with the RFID-Stakeholders Group, is expected to stimulate and to steer this process of self-regulation. In this context, the EDPS welcomes the Recommendation announced in the Communication which is expected to contain specific guidelines setting up '*the principles that public authorities and other stakeholders should apply in respect of RFID usage*'.

37. The Communication foresees that self-regulation takes the form of a code of conduct or a code of good practice. According to the EDPS, independently of whatever form the self-regulation takes, it should:

— provide concrete and practical guidance on specific types of RFID applications and hence contribute to compliance with the data protection legal framework,

— deal with the specific data protection questions and problems that arise in the context of generic RFID applications,

— contribute to the uniform and harmonised application of the Data Protection Directive throughout the EU, precisely in a sector that is likely to use the same type of RFID applications across the EU,

— be applied by all relevant stakeholders. Non-compliance should have negative (possibly financial) consequences.

38. The EDPS points at one issue where self-regulation will be specifically useful. For those RFID applications that entail the processing of personal data, the Data Protection Directive imposes upon data controllers various obligations, in particular under Article 17 (security of processing) and under Article 7 (the need to process data only with the appropriate legal grounds). Pursuant to these provisions, data controllers must on the one hand set up measures against the unauthorised disclosure of the data. On the other hand, data controllers must ensure that the processing, such as disclosure of information through the readers, where appropriate, only occurs with the informed consent of the individual to whom the data refers.

39. These provisions of the Data Protection Directive can be interpreted as requiring that RFID applications are deployed with the necessary technical solutions to prevent or minimise the risks of unwanted disclosure and ensure that the processing or transfer of data only happens with informed consent, where appropriate. In the EDPS's view, the existence of such an obligation (i.e. to apply necessary technical solutions to prevent or minimise the risks of unwanted disclosure) and its binding nature upon deployers of RFID applications, will be even stronger and clearer if this requirement is taken up in the forthcoming code of conduct or code of good practice mentioned above. For these reasons, the EDPS strongly advises that the Commission's Recommendation includes such an interpretation of the Data Protection Directive, underlining the existence of an obligation to deploy RFID applications with the necessary technological measures to prevent the unwanted collection or disclosure of information.

The need for guidance

40. The EDPS recommends that the Commission, in close cooperation with the RFID Expert Group, will produce one or more documents giving clear guidance how to apply the current legal framework to the RFID environment. The guidance should foresee practical ways how the principles set out in the Data Protection Directive and the ePrivacy Directive are complied with. As for the overall approach of the guidance and its concrete content, the EDPS has the following suggestions.

41. The guidance setting out the principles that apply in respect of RFID usage should be sufficiently focussed and adopt a sector specific approach. A 'one size fits all' approach will not fulfil the purposes sought of ensuring a clear and coherent framework. Instead, the scope of the guidance must be limited to well-defined RFID sectoral applications.

42. Furthermore, the guidelines should propose practical and efficient methods for developing *techniques and standards* which could contribute to the RFID systems' compliance with the data protection legal framework and which will entail the use of 'privacy by design' technology.

43. In applying the current legal framework to the RFID environment, particular attention must be paid to the application of the data protection principles and obligations that apply to data controllers of RFID applications. Particularly relevant are the following obligations and principles:

— the right to information principle, including the right to know when data are collected through readers, and in appropriate cases that products are tagged,

— the notion of consent as one of the legal grounds to process data. This notion materialises in the obligation to deactivate RFID tags at the point of sale, unless the data subject has given his or her consent ([1]). The right to deactivate RFID tags also serves the purposes of ensuring the security of the information, i.e. to ensure that the data processed through RFID tags is not disclosed to unwanted third parties,

— the right of individuals not to be subject to adverse decisions based solely on the automated processing of a defined personal profile.

44. As far as the right to information is concerned, the guidance should establish that individuals must be provided with *information* regarding the processing of their personal data. In particular they should be alerted, among others, of (i) the presence of readers and the presence of activated RFID tags on products or their packaging; (ii) the consequences of such presence in terms of information gathering; and (iii) the purposes for which the information collected is intended to be used.

45. The use of logos may be suitable as a measure to provide information. Logos may be used to alert of the presence of readers and RFID tags which are supposed to remain active. However, the use of logos alone will not be sufficient to ensure the fair processing of information which requires the information to be provided to data subjects in a clear and comprehensible manner. The use of logos should be considered as a measure to supplement the provision of more detailed information.

([1]) See, more in detail, paragraphs 46-50 of this Opinion.

The cornerstone: The Opt-in principle

46. For all relevant RFID-applications, solutions should respect and implement as a prerequisite, an opt-in principle at the point of sale. Enabling the RFID tags to continue transmitting information after the point of sale would be unlawful unless the data controller had appropriate legal grounds. Appropriate legal grounds would normally only be (a) the consent of the data subject or (b) if such disclosure was necessary in order to deliver a service, a specific and free request by the said individual ([1]). Both legal grounds would then qualify as 'opt in'.

47. Under the opt-in principle, tags should be deactivated at the point of sale unless the individual who bought the product to which the tag is attached wanted to leave it active. By exercising the right to leave it active, the individual would be consenting to the further processing of his or her data, for example, to the transmission of the data to the reader at his or her next visit to the data controller.

48. In order to cope with the growing diversity of RFID applications and to facilitate the development of new innovative business models, the EDPS stresses the importance of a flexible approach. Flexibility has to be provided as to the implementation of the opt-in principle.

49. The options to implement the opt-in principle are multiple. For example, as an alternative to the removal of the tag, it could be envisaged that the tag would be blocked, temporarily disabled or following a security policy model called resurrecting duckling model ([2]), locked to a specific user. In the case of tag with a short life cycle, the address of the tag which pinpoints to information stored in a database could also be erased from the reference database avoiding further processing of additional data collected by the tag.

50. To conclude, although the EDPS argues that the 'opt-in-principle' at the point of sale is a legal obligation that already exists under the Data Protection Directive in most situations, there are good reasons to specify this obligation in self-regulatory instruments, also in order to ensure that the principle will be implemented in the most appropriate way. Specific implementation is in any event needed for those RFID applications that fall outside of the scope of the Data Protection Directive.

([1]) In some RFID-applications, it may be possible to rely on other grounds, such as Article 7(f) (legitimate interests of the controller, subject to adequate safeguards).

([2]) The name of this model developed by Frank Stajano and Ross Anderson from the University of Cambridge was inspired by 'how a goose hatchling assumes that the first moving object it sees must be its mother'.

The need for 'privacy by design'

51. In order to minimise privacy and data protection threats, the Commission's Communication endorses in part 3.2, page 6, the idea of the specification and adoption of early design criteria. The EDPS welcomes this approach. Indeed, the adoption of specifications and design criteria, otherwise referred to as Best Available Techniques ('BATs'), will efficiently contribute to data protection regulation and security requirements. This identification of technological and organisational criteria, if frequently reviewed, will strengthen the symbiosis model of privacy and security requirements the European Union is developing.

52. The proper definition of privacy and security BATs for RFID systems will also be decisive for building a trustworthy environment which will reinforce their wide acceptance by end users, as well as for the European industry's competitiveness.

53. The process of selecting BATs for RFID systems should be fuelled by privacy and security impact assessments for which efforts still need to be invested. The EDPS considers that the European Network and Information Security Agency (ENISA) together with the Joint Research Centres of the European Commission associated with the relevant industry stakeholders can contribute to the identification of these best practices and to the development of such methodologies. By launching recently the project 'technical Guidelines RFID', the German Federal Office for Information Security (BSI) gave a proper illustrative example ([3]) of BATs which should be developed now at the European level.

54. Standards can also play a decisive role in the early adoption of the privacy-by-design principle. The Commission should therefore contribute to the adoption of privacy and data protection safeguards in the development of international RFID standards. The Article 29 Working Party in its working document ([4]) on RFID clearly illustrated the possibility for standards to contribute to the privacy friendly development of RFID systems.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Working document (WP 105) on data protection issues related to RFID technology, 19 January 2005.

55. Furthermore, the EDPS welcomes the position adopted by the Commission regarding research and development of RFID technologies and the need to mitigate privacy risks. Indeed, the privacy-by-design principle needs to be introduced at the earliest stage of the development of technologies which will better contribute to their compliance with the data protection legal framework. The EDPS, as briefly presented in his Annual Report 2006 will associate himself to this effort by providing, on a case-by-case basis, opinions and advices to projects of the 7th Framework Programme (2007-2013).

V. **ARE SPECIFIC LEGISLATIVE MEASURES NEEDED?**

56. Self-regulation may not be enough as a means for full implementation of the existing framework for data protection and privacy. Even if the self-regulation fulfils the requirements mentioned above, its application is voluntary and its non-compliance can not always be effectively sanctioned. Additionally, binding legislative measures may still be needed, in order to ensure the protection of individuals' rights to privacy and data protection. This is all the more needed in case of failure of the self-regulated approach.

57. A key question is the determination of the legal instruments necessary to ensure that RFID applications are effectively deployed with the necessary technical solutions to prevent or minimise the risks for data protection and privacy, and that responsible controllers take adequate measures to comply with their obligations under existing legal frameworks. This raises some additional questions:

— are specific rules needed?

— if so, can these rules be adopted within the existing legislative framework, for instance by making use of existing comitology-procedures?

— or is a new legislative instrument necessary to ensure the effective deployment of RFID application with embedded privacy enhancing technologies?

58. This chapter will address the possibilities of issuing binding legislative measures within the existing legal framework, whereas Chapter VI will discuss, because it is a separate issue, the need for a new legislative instrument.

59. In the first place, specific attention should be given to the provisions of Article 17 of Directive 95/46/EC, Article 14(3) of Directive 2002/58/EC and Article 3(3)(c) of Directive 1999/5/EC. Article 14(3) allows Member States to adopt measures to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC [1]. Directive 1999/5/EC provides in its Article 3(3)(c) that the Commission may decide — with a comitology procedure — that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected. Article 3(3)(c) of Directive 1999/5/EC has not been used until now.

60. These provisions give the legislator — on the national and on the Community level — the power to prescribe that privacy and data protection safeguards must be included in the manufacturing of RFID systems, a concept that is known as 'privacy by design' [2]. It calls also for the use of Best Available Techniques.

61. In order to make the use of the concept of 'privacy by design' compulsory, the EDPS recommends that the Commission uses the mechanism of Article 3(3)(c) of Directive 1999/5/EC, in consultation with the RFID Expert Group.

62. In the second place, it is possible to specify the application of the existing legislative framework to RFID, by modifications of the directives themselves. As said, the Commission has just presented a proposal for amending the ePrivacy Directive which contains a new provision with this perspective. The EDPS welcomes this first confirmation of the applicability of the Directive to RFID applications. The EDPS will deal with specific issues raised by the relation between the ePrivacy Directive and RFID in his opinion on the proposal for amendment, which will be issued early in 2008.

63. Taking into account that the Commission does not foresee any modification of the Data Protection Directive in the near future [3], the possibilities for specification relating to the application of the existing legislative framework to RFID are limited.

VI. **IS A SPECIFIC LEGAL FRAMEWORK ON RFID NEEDED?**

Intentions of the Commission

64. The Communication [4] emphasises the importance of security and privacy-by-design. It also requires involvement of all stakeholders. The main result of the activities of the Commission will be *'a Recommendation to set out the*

[1] And in accordance with Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications (OJ L 36, 7.2.1987, p. 31).
[2] See Chapter IV.
[3] The EDPS supports this approach, see point 64.
[4] See paragraph 4.1 of the Communication.

principles that public authorities and other stakeholders should apply in respect of RFID usage'. The Recommendation will probably be adopted in spring 2008. The legislative ambitions mentioned in the Communication contain two steps. The Commission will:

— Consider appropriate provisions on RFID in the forthcoming proposal for an amendment of the ePrivacy Directive. As said before, the Commission has proposed such an amendment of the ePrivacy Directive in November 2007, confirming the applicability of the Directive to RFID applications ([1]), but not proposing widening the scope of the ePrivacy Directive to private networks.

— Assess the need for further legislative steps to safeguard data protection and privacy.

65. Following this policy, it can be expected that the Commission does not envisage — at least not on a short term — proposing new specific legislation to safeguard data protection and privacy in the area of RFID.

Parameters for the legislator

66. In his Opinion on the Communication on the Data Protection Directive, the EDPS listed some outlines for legislative activities relating to the processing of personal data which can be summarized as follows:

— firstly, the core principles of data protection should be kept: '*There is no need for new principles, but there is a clear need for other administrative arrangements, which are on the one hand effective and appropriate to a networked society and on the other hand minimise administrative costs*' ([2]),

— secondly, legislative proposals should only be submitted if the necessity and proportionality are sufficiently demonstrated. For this reason, on the short term the general legislative framework for data protection should not be changed,

— thirdly, changing developments in society may lead to specific legal frameworks, in order to adapt the principles of the Data Protection Directive to issues raised by specific technologies such as RFID. It is clear that also in this context the conditions of necessity and proportionality need to be fulfilled.

67. As a next step it is useful to specify the expectations the legislator has to face in the area of RFID:

— legislation needs to be flexible and leave room for innovations and technological development. This should lead to legislation that is sufficiently technology neutral,

— in the second place, legislation needs to provide for legal certainty. This should lead to legislation that is sufficiently specific. Stakeholders must know precisely how their behaviour is regulated,

— in the third place, legislation must effectively protect all justified interests at stake. This requires in any event enforcement of the legislation and clear definition of responsibilities: which party is accountable for what behaviour ([3])? These requirements are even more predominant where privacy and data protection are at stake, fundamental rights of the individual under the European Convention of Human Rights and Fundamental Freedoms and the Charter of the Fundamental Rights of the European Union.

Point of view of the EDPS

68. To the EDPS, it is clear that not all technological developments should lead to reactions by the European legislator. Technological developments can go fast, whereas the adoption and entry into force of legislation takes time and should take time. Legislation should be the result of balancing all the interests at stake. When the instrument of a directive is chosen, even more time is needed, since directives must be fully implemented in the legal systems of the Member States.

69. However, RFID is not just another technological development as has been underlined in several parts of this opinion. The Communication refers to RFID as the gateway to a new phase of development of the Information Society, often referred to as the 'internet of things' and RFID tags will constitute key elements of the 'ambient intelligent' environments. These environments are also important steps in the development of what is often called the 'Surveillance Society' ([4]). Against this background, legislative action in the area of RFID can be justified. RFID may bring about a qualitative change.

([1]) See proposed new Article 3 of Directive 2002/58/EC.
([2]) Point 24 of the Opinion on the Communication on the Data Protection Directive.
([3]) Put in data protection terminology this implies the identification of the 'data controller'.
([4]) This message was repeated in a statement of the European data protection authorities adopted in London on 2 November 2006 available at EDPS website: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. In this perspective, the EDPS recommends considering the adoption of (a proposal for) Community legislation regulating the main issues of RFID-usage in relevant sectors, in case the proper implementation of the existing legal framework would fail. After it enters into force, such a legislative measure must be considered as a *lex specialis vis-à-vis* the general data protection framework.

71. Adoption of such a legislative instrument would have the following advantages:

— the instrument could set the substantive parameters for the self-regulatory mechanisms,

— the perspective of the adoption of a legislative instrument might prove to be an effective incentive for stakeholders to set up self-regulatory mechanisms offering accurate protection.

72. To make it more practical, the Commission could be asked to prepare a consultation document on the pros and cons of specific legislation, and of the main elements of such legislation. Of course, the stakeholders could be asked to give input to this consultation. Likewise, the Article 29 Working Party could be involved.

Possible modalities

73. The intervention of the legislator could provide for a tailor made legal framework, which consists of a mix of regulatory tools which specify and complement the existing legal framework. This tailor made legal framework should be based on the known principles of data protection and should focus on the division of responsibilities and on the effectiveness of control mechanisms.

74. A specific reason for which such tailor made legislation might be needed relates to the fact that not all RFID applications entail the processing of personal data. In other words, if RFID applications do not entail the processing of personal data, parties involved in the manufacturing and selling of RFID enabled products are not legally bound to implement any technological measures that would prevent eavesdropping or the setting up of readers without proper notice to individuals. Yet, as demonstrated, privacy risks derived from the possible surveillance of individuals also exist for such RFID applications, thus demanding the same type of privacy safeguards. Precisely, this may be the case for item level tagging in consumer products *before* the point of sale. In sum, RFID applications that do not process personal data may still threaten individuals' privacy by enabling surreptitious surveillance and the use of the information for unacceptable purposes.

75. The EDPS considers that this unfortunate outcome should be avoided. Because current legislation partially — at least for RFID applications that do not process personal data — fails to counter this privacy threat, and taking into account the shortcomings of soft law solutions, it seems necessary to use compulsory legislative measures to ensure a satisfactory result.

76. Such measures should in any event:

— lay down the opt-in principle at the point of sale as a precise and undeniable legal obligation, also for RFID applications that fall outside of the scope of the Data Protection Directive ([1]),

— ensure the mandatory deployment of RFID applications with the appropriate technical features or 'privacy by design'.

VII. **THE ISSUE OF GOVERNANCE**

77. Although the 'inherently trans-border' dimension of RFID systems is seen in the Communication only within the Internal Market, the EDPS considers that this dimension has to be tackled at a more international level. In a shop, RFID systems are already 'trans-border' as the activity of the tag might not stop at the point of sale. At the level of the overall RFID system, these technologies also become 'trans-border' when transfer of personal data to a third country might take place as the producer of the tagged item, which is part of the RFID system, is based outside the European Union ([2]).

78. From a more prospective point of view, the governance of RFID identity reference databases also represents a critical dimension for appropriate enforcement of the European data protection legal framework. The EDPS urges for a solution to be found as further erosion of this framework would not be acceptable.

79. The EDPS foresees the RFID governance issue as a major challenge which will request considerable investments. The right forum of negotiation as well as the most appropriate management infrastructure will have to be found in order to ensure that data protection rights are adequately respected in these international environments.

([1]) Chapter IV has argued that the 'opt-in' principle at the point of sale is a legal obligation that already exists under the Data Protection Directive.

([2]) The obligations surrounding transfer of personal data are dealt with in Articles 25 and 26 of the Data Protection Directive.

80. In this perspective, the EDPS invites the Commission to present its views on the issue of governance, possibly in consultation with the RFID-Stakeholders Group.

VIII. **CONCLUSION**

81. The EDPS welcomes the Commission's Communication on RFID as it tackles the main issues arising in the context of the deployment of RFID technology without neglecting the determinant ones related to privacy and data protection. He agrees with the view that RFID systems could play a key role in the development of the Information Society usually referred to as the 'Internet of things'.

Clarifying the consequences

82. The wide use of RFID-technology is fundamentally new and may have a fundamental impact on our society and on the protection of fundamental rights in our society, such as privacy and data protection. RFID may bring about a qualitative change.

83. Five basic privacy and security issues can be distinguished:

— the identification of the data subject,

— the identification of the data controller(s),

— the decrease meaning of the traditional distinction between the personal and the public sphere,

— the consequences of the size and the physical properties of RFID-tags,

— the lack of transparency of the processing.

Specifying the consequences

84. The general legislative framework for data protection as laid down in Directive 95/46/EC applies to RFID, as far as data processed by RFID systems fall within the definition of personal data.

85. As far as the ePrivacy Directive is concerned: the Commission Proposal of 13 November 2007 for amendment of the Directive contains a provision aiming to specify that the Directive indeed applies to certain RFID applications. However, other certain RFID-applications might not be covered because of the limitation of this Directive to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

86. The protection of personal data can be complemented by a range of self-regulatory instruments. It is appropriate to leave room for such self-regulation, provided that:

— it provides concrete and practical guidance on specific types of RFID applications,

— it deals with the specific data protection questions and problems that arise in the context of generic RFID applications,

— it contributes to the uniform and harmonised application of the Data Protection Directive throughout the EU,

— it is applied by all relevant stakeholders

87. The EDPS recommends that the Commission, in close cooperation with the RFID Expert Group, will produce one or more documents giving clear guidance how to apply the current legal framework to the RFID environment.

88. The guidance setting out the principles that apply in respect of RFID usage should be sufficiently focussed and adopt a sector specific approach. It should propose practical and efficient methods for developing *techniques and standards* which could contribute to the RFID systems' compliance with the data protection legal framework and which will entail the use of 'privacy by design' technology.

89. The EDPS welcomes the approach in the Commission's Communication to endorse the idea of the specification and adoption of early design criteria.

90. Although the EDPS considers the 'opt-in' principle at the point of sale is a legal obligation that already exists under the Data Protection Directive in most situations, this obligation should be specified in self-regulatory instruments.

Are specific measures needed?

91. In order to make the use of the concept of 'privacy by design' compulsory, the EDPS recommends that the Commission uses the mechanism of Article 3(3)(c) of Directive 1999/5/EC, in consultation with the RFID Expert Group.

92. The EDPS recommends considering the adoption of (a proposal for) Community legislation regulating the main issues of RFID-usage in relevant sectors, in case the proper implementation of the existing legal framework would fail. After it enters into force, such a legislative measure must be considered as a *lex specialis vis-à-vis* the general data protection framework. This legislative measure should also address the privacy and data protection concerns that arise in certain RFID applications, such as item level tagging before the point of sale, which may not necessarily involve the processing of personal data.

93. The Commission should prepare a consultation document on the pros and cons of specific legislation, and of the main elements of such legislation.

94. The intervention of the legislator could provide for a tailor made legal framework, which consists of a mix of regulatory tools which specify and complement the existing legal framework. Measures should in any event:

— lay down the opt-in principle at the point of sale as a precise and undeniable legal obligation, also for RFID applications that fall outside of the scope of the Data Protection Directive ([1]),

— ensure the mandatory deployment of RFID applications with the appropriate technical features or 'privacy by design'.

The issue of governance

95. The EDPS invites the Commission to present its views on the issue of governance, possibly in consultation with the RFID-Stakeholders Group.

Done at Brussels, 20 December 2007.

Peter HUSTINX

European Data Protection Supervisor

([1]) Chapter IV has argued that the 'opt-in-principle' at the point of sale is a legal obligation that already exists under the Data Protection Directive.