Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 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, as last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009,

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. Information and communication technologies (ICT) are enabling tremendous capabilities in virtually every aspect of our lives - how we work, play, socialize and educate. They are essential for today's information economy and for society in general.

2. The European Union is a global force in advanced ICT and is determined to remain so. To meet this challenge, the European Commission is soon expected to adopt a new European Digital Agenda which Commissioner Kroes has confirmed as her priority[1].

[1] Answers to European Parliament Questionnaire for Commissioner Neelie Kroes in the context of the EP hearings that preceded the Commissioner's designation.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

3. The EDPS acknowledges the benefits that arise from ICT and agrees that the EU should do its utmost to boost their development and widespread adoption. He also fully endorses the views of Commissioners Kroes and Reding that individuals should be at the core of this new environment[2]. Individuals should be able to rely on ICT's ability to keep their information secure and control its use, as well as be confident that their privacy and data protection rights will be honored in the digital space. Respect of those rights is essential in order to generate consumer trust. And such trust is crucial if citizens are to embrace new services[3].

4. The EU has a strong data protection/privacy legal framework, the principles of which remain completely valid in the digital age. However, one cannot be complacent. In many instances, ICT raise new concerns that are not accounted for within the existing framework. Some action is therefore necessary to ensure that individual rights, as enshrined in EU law, continue to provide effective protection in this new environment.

5. This Opinion discusses the measures that could be either promoted or undertaken by the European Union in order to guarantee individuals' privacy and data protection in a globalised world that will remain technologically driven. It discusses legislative and non legislative instruments.

6. After providing an overview of ICT as a new development that creates opportunities but also risks, the Opinion discusses the need to integrate, at practical level, data protection and privacy from the very inception of new information and communication technologies (which is referred to as the principle of "Privacy by Design"). In order to compel compliance with this principle, the Opinion discusses the need to provide for the principle of "privacy by design" into the data protection legal framework in at least two different ways. First, by incorporating it as a general, binding principle and, second, by incorporating it in particular ICT areas, presenting specific data protection/privacy risks which may be mitigated through adequate technical architecture and design. These areas are Radio Frequency Identification (RFID), social network applications and browsers applications. Finally, the Opinion makes suggestions regarding other tools and principles aiming at protecting individual's privacy and data protection in the ICT sector.

7. In addressing the above, the opinion elaborates on some of the points made by the Article 29 Working Party in its contribution to the public consultation on the future of privacy[4]. It furthermore builds on earlier opinions of the EDPS, such as the Opinion of 25 July 2007 on the implementation of the Data protection Directive, the Opinion of 20 December 2007 on RFID and his two opinions on the ePrivacy Directive.[5]

---

[2] Answers to European Parliament Questionnaire for Commissioner Neelie Kroes in the context of the EP hearings that preceded the Commissioner's designation; Commissioner Viviane Reding's speech on "A European Digital Agenda for the New Digital Consumer, delivered at BEUC Multi-stakeholder Forum on Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives", Brussels 12 November 2009.

[3] See, for example, RISEPTIS Report, "Trust in the Information Society", A Report of the Advisory Board, RISEPTIS (Research and Innovation on Security, Privacy and Trustworthiness in the Information Society). Available at http://www.think-trust.eu/general/news-events/riseptis-report.html. See also:
J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No. 1

[4] Article 29 Working Party Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009.

[5] Opinion of 25 July 2007 on 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, OJ C 255, 27.10.2007, p. 1; Opinion of 20 December 2007 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), OJ C 101,

II. ICT OFFER NEW OPPORTUNITIES BUT PRESENT ALSO NEW RISKS

8. ICT have been compared to other important inventions of the past, such as electricity. While it may be too early to assess their real historical impact, the link between ICT and economic growth in developed countries is clear. ICT have created employment, economic benefits and contributed to overall welfare. The impact of ICT goes beyond the purely economic, since it has played an important role in boosting innovation and creativity.

9. Furthermore, ICT have transformed the way people work, socialise and interact. For example, people increasingly rely on ICT for social and economic interactions. Individuals can make use of a wide range of new ICT applications such as eHealth, eTransport, eGoverment as well as innovative interactive systems for entertainment and learning.

10. In the light of such benefits, the European Institutions have all expressed their commitment to support ICT as a necessary tool to improve the competitiveness of European industry and to accelerate Europe's economic recovery. Indeed, in August 2009 the Commission adopted the Europe's Digital Competitiveness Report[6] and launched a public consultation on appropriate future strategies to boost ICT. On 7 December 2009, the Council put forward a contribution to this consultation, entitled "Post i2010 Strategy - Toward an open, green and competitive knowledge society"[7]. The European Parliament has just adopted a report intended to provide guidance to the Commission in defining a digital agenda [8]

11. With the opportunities and benefits that accompany the development of ICT come new risks, particularly for the privacy and protection of personal data of individuals. ICT often lead to a proliferation (quite often in ways that are out of sight to individuals) in the amount of information that is collected, sorted, filtered, transferred or otherwise retained, and the risks to such data therefore multiply.

12. For example, RFID chips are replacing barcodes on (some) consumer products. By improving the information flow in the supply chain (and thus reducing the need for "safety" stocks, providing more accurate forecasts, etc) the new system is supposed to benefit business and consumers alike. However, at the same time, this raises the disturbing possibility of being tracked, for different purposes and by different entities, through tagged personal possessions.

13. Another example is "cloud computing", essentially the delivery of hosted consumer and non-consumer application services over the Internet. These range from photo libraries, calendars, webmail and customer databases to more complex business-related services. The benefits for both businesses and individuals are clear; cost reduction (costs are incremental), location-less (easy access to information anywhere in the world), automation (no need for dedicated IT resources, and to keep software up to date) etc. At

---

23.04.2008, p. 1; Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ C 181, 18.07.2008, p. 1; Second opinion of 9 January 2009 on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications.

[6] Europe's Digital Competitiveness Report- Main achievements of the i2010 strategy 2005-2009,{SEC (2009) 1060}.

[7] Council Conclusions "Post i-2010 Strategy-- Towards and Open, Green and Competitive Knowledge Society. (17107/09), adopted on 18.12.2009.

[8] Report on defining a new Digital Agenda for Europe: from i2010 to digital.eu (2009/2225 (INI)), adopted on 18.03.2010.

the same time, the risks of security glitches and hacking exist and are very real. There is also the concern of losing access to and control over one's own data.

14. Benefits and risks have been shown to coexist in other areas using ICT applications. Take eHealth, which can enhance effectiveness, reduce costs, increase accessibility and generally improve the quality of healthcare services. However, eHealth often raises the issue of the legitimacy of secondary uses of eHealth information, requiring a careful analysis of the purposes of any potential secondary use[9]. Furthermore, as electronic health records have become more widely used, the systems themselves have been dogged by scandals revealing many cases of hacking into electronic health records.

15. In sum, some degree of residual risk is likely to persist, even after making the right assessments and applying the necessary measures. A situation of zero risk would be unrealistic. However, as further discussed below, measures can and must be implemented to reduce such risk to appropriate levels.

III. PRIVACY BY DESIGN AS A KEY TOOL FOR GENERATING INDIVIDUAL TRUST IN ICT

16. The potential benefits of ICT can only be enjoyed in practice if they are able to generate trust, in other words, if they can secure user willingness to depend on ICT because of their characteristics and benefits. Such trust will only be generated if ICT are reliable, secure, under individuals' control and if the protection of their personal data and privacy is guaranteed.

17. Widespread risks and failures such as those illustrated above, particularly when they entail the misuse or breaches of personal data exposing the privacy of individuals, are likely to endanger user trust in the information society. This could seriously jeopardise the development of ICT and the benefits they could bring.

18. However, the solution to these risks to privacy and data protection cannot be to eliminate, exclude or refuse to use or promote ICT. This would be neither feasible nor realistic; it would prevent individuals from enjoying the benefits of ICT and would seriously limit the overall advantages to be gained.

19. The EDPS believes that a more positive solution is to design and develop ICT in a way that respects privacy and data protection. It is therefore crucial that privacy and data protection are embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal. This is usually referred to as "privacy by design" (PbD) and is further discussed below.

20. PbD can entail different actions, depending on the particular case or application. For example, in some cases it may require eliminating/reducing personal data or preventing unnecessary and/or undesired processing. In other cases, PbD may entail offering tools to enhance individuals' control over their personal data. Such measures should be considered when standards and/or best practices are defined. They can also be incorporated into the architecture of information and communication systems, or in the structural organisations of the entities that process personal data.

[9] For example, selling or using health information collected for the purposes of providing treatment may not be used to select sites for satellite clinics, to establish ambulatory surgery canters, and in other ways to plan future activities with financial implications would require careful examination.

III.1. Privacy by design principle applicable in different ICT environments and their impact

21. The need for the principle of PbD can be found in many different ICT environments. For example, the healthcare sector increasingly relies on ICT infrastructures which often entail centralised storage of patients' health related information. The application of the PbD principle in the health sector would require assessing the suitability of different measures such as the possibility of minimising data stored centrally or limiting it to an index, using encryption tools, assigning access rights strictly on 'a need to know basis', anonymising data once they are no longer required, etc

22. Similarly, transport systems are increasingly provided by default with advanced ICT applications that interact with the vehicle and its environment for different purposes and functions. For example, cars are increasingly equipped with new ICT functionality (GPS, GSM, network of sensors, etc.) providing not only their location but also their technical conditions in real time. This information could be used, for example, to replace the existing road tax system by a usage-dependent road charge. The application of PbD to the design of the architecture of such systems should support the processing and onward transfer of as little personal data as possible[10]. In keeping with this principle, decentralised or semi-decentralised architectures limiting the disclosure of location data to a central point would be preferable to centralised ones.

23. The above examples show that when information and communication technologies are built according to the principle of PbD, the risks to privacy and data protection may be significantly minimised.

III.2. Not enough deployment of ICT applying PbD

24. An important question is whether economic operators, ICT manufacturers/providers and data controllers are interested in marketing and implementing the PbD principle in ICT. In this context, it is also important to assess user demand for PbD.

25. In 2007, the Commission issued a communication calling upon businesses to use their power of innovation to create and implement PETs as a way to improve the protection of privacy and personal data from the very beginning of the development cycle[11].

26. To date however, the available evidence shows that neither ICT manufacturers nor data controllers (in either the private or public sector) have managed to consistently implement or market PbD. Different motivations have been adduced, including lack of economic incentives or institutional support, insufficient demand, etc[12].

27. At the same time, user demand for PbD has been rather low. Users' of ICT products and services may rightly assume that their privacy and personal data are *de facto* protected,

---

[10] See Opinion of the European Data Protection Supervisor of 22 July 2009 on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, available at:
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf.

[11] Communication of 2.5.2007. COM (2007) 228 final from the Commission to the European Parliament and the Council on promoting data protection by privacy enhancing technologies (PETs).

[12] Study on the economic benefits of privacy enhancing technologies (PETS) jls/2008/D4/036.

when in many cases, they are not. In some cases, they are simply not in a position to take the security measures necessary to protect either their own personal data or those of others. In many instances this is because they lack the full or even partial knowledge of the risks. For example, generally speaking young people disregard the privacy risks associated with displaying personal information on social networks and often ignore privacy settings. Still other users are aware of the risks but may not have the necessary technical expertise to implement safeguarding technologies, such as those that protect their Internet connection or how to amend browser settings to minimise profiling based on the monitoring of their websurfing activities.

28. Yet, the risks to the protection of privacy and data protection are very real. If privacy and data protection are not taken into account from the start, it is often too late and economically too cumbersome to fix the systems, and too late to repair the harm already done. The increasing number of data breaches in recent years perfectly illustrates this problem and reinforces the need for privacy by design.

29. The above clearly suggests that manufacturers and providers of ICT technologies designed to process personal data should have, together with data controllers, a responsibility to design them with inbuilt data protection and privacy safeguards. In many instances this would mean that they should be designed with privacy by default settings.

30. Against this backdrop, we need to consider what steps should be taken by policy makers to promote PbD in the development of ICT. A first question is whether the existing legal data protection framework contains adequate provisions to ensure the implementation of the principle of PbD by both data controllers and manufacturers/developers. A second question is what should be done in the context of the European Digital Agenda to ensure that the ICT sector generates consumer trust.

IV. EMBEDDING THE PRINCIPLE OF PRIVACY BY DESIGN IN EU LAWS AND POLICIES

IV.1. The current data protection and privacy legal framework

31. The EU has a robust data protection and privacy framework enshrined in Directive 95/46/EC[13], Directive 2002/58/EC[14] and the jurisprudence of the European Court of Human Rights[15] and the Court of Justice.

32. The data protection Directive applies to *"any operation or set of operations which is performed upon personal data*" (collection, storage, disclosure, etc.). It imposes compliance with certain principles and obligations upon those who process personal data ('data controllers'). It sets forth individual rights, such as the right to access personal information. The ePrivacy

[13] 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**,** OJ 1995, L 281/31 (further: Data protection Directive).

[14] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ 2002, C 201/37, as last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337/11. fields (further: ePrivacy Directive).

[15] Interpreting the main elements and conditions set out in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) adopted in Rome on 4 November 1950, as they apply to different.

Directive deals specifically with the protection of privacy in the electronic communication sector.[16]

33. The current data protection Directive does not contain an explicit requirement for PbD. However, it includes provisions which indirectly, in different situations, may well demand the implementation of the principle of PbD. In particular, Article 17 requires that data controllers implement appropriate technical and organization measures to prevent unlawful data processing[17]. PbD is therefore covered in a very generic way. Furthermore, the provisions of the Directive are mainly addressed to data controllers and their processing of personal information. They do not explicitly require that information and communications technologies are privacy and data protection compliant, which requires also addressing designers and manufacturers of ICT, including the activities carried out at the stage of standardization.

34. The ePrivacy Directive is more explicit. Article 14.3 provides that "*Where required, measures may be adopted 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 and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications)*". However, this provision has never been used[18].

35. Whereas the above provisions of the two Directives are helpful towards the *promotion* of privacy by design, in practice they have not been sufficient in *ensuring* that privacy is embedded in ICT.

36. As a result of the above situation, the law does not in a sufficiently precise way require that ICT is designed in accordance with the principle of PbD. Also, data protection authorities do not have enough powers to ensure imbedding PbD. This results in ineffectiveness. For example, data protection authorities may be able to impose sanctions for failure to answer to access requests made by individuals and they will have the competences to require the implementation of certain measures to prevent unlawful data processing. Yet it is not always sufficiently clear whether their powers extend to requiring a system to be designed in a way that facilitates individuals' data protection rights[19]. For example, on the basis of the existing legal provisions it is unclear whether it could be required that the architecture of an information system is designed in a way that facilitates the companies' response to access requests made by individuals so that such requests can be handled automatically and quicker. Furthermore, later attempts to alter the technology once it has been developed or deployed may result in a patchwork of solutions that do not fully work, besides being economically onerous.

---

16 The Lisbon Treaty has reinforced such protection by recognising the respect for private life and protection of personal data as separate fundamental rights in Article 7 and 8 of the EU Charter of fundamental rights. The EU Charter of Fundamental became binding when the Lisbon Treaty entered into force.

17 Article 17 reads as follows: "*Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*". Recital 46 complements it by saying "*Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing*".

18 The Commission has announced plans to update Directive 1999/5/EC towards the end of 2010.

19 See Report of the UK Information Commissioner's Office entitled: "Privacy by Design", published in November 2008.

37. In the EDPS' view, which is shared with the Article 29 Working Party[20], the current legal framework leaves room for a more explicit endorsement of the principle of PbD.

IV.2. Embedding Privacy by Design on different levels

38. In the light of the above, the EDPS recommends the Commission to follow four courses of action:
    a) Propose to include a general provision on PbD in the legal framework for data protection.
    b) Elaborate this general provision in specific provisions, when specific legal instruments in different sectors are proposed. These specific provisions could already now be included in legal instruments; on the basis of Article 17 of the Data Protection Directive (and other existing law).
    c) Include PbD as a guiding principle in Europe's Digital Agenda.
    d) Introduce PbD as a principle in other EU-initiatives (mainly non legislative).

A general provision on PbD

39. The EDPS proposes to include unequivocally and explicitly the principle of privacy by design into the existing data protection regulatory framework. This would make the principle of PbD stronger, more explicit, and it will compel its effective implementation, in addition to giving more legitimacy to enforcement authorities to require its *de facto* application in practice. This is particularly necessary in the light of the facts outlined above, not only the importance of the principle itself as a tool to foster trust, but also as an incentive to stakeholders to implement PbD and enhance the guarantees that are provided for in the existing legal framework.

40. This proposal builds on the Article 29 Working Party's recommendation to introduce the principle of 'privacy by design' as a general principle in the data protection legal framework, in particular, in the Data Protection Directive. According to the Article 29 Working Party: "*This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements*".

41. The EDPS also welcomes Commissioner Viviane Reding's endorsement of the privacy by design principle made in the context of announcing the review of the Data Protection Directive[21].

42. This leads to the content of such regulation. First and most important, a general privacy by design principle should be technologically neutral. The principle should not intend to regulate technology, i.e. it should not prescribe specific technical solutions. Instead, it should mandate that existing privacy and data protection principles be integrated into information and communication systems and solutions. This would allow stakeholders, manufacturers, data controllers and DPAs, to interpret the meaning of the principle in

[20] See Article 29 Working Party Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1st December 2009.

[21] 'Privacy by design is a principle that is in the interest of both citizens and businesses. Privacy by design will lead to better protection for individuals, as well as to trust and confidence in new services and products, that will in turn have a positive impact on the economy. There are some encouraging examples but much more needs to be done. Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels.

each individual case. Second, compliance with the principle should be mandatory at different stages, from the creation of standards and the design of the architecture to their implementation by the data controller.

Provisions in specific legal instruments

43. Current and forthcoming legislative instruments must integrate the principle of PbD on the basis of the current legal framework, and, after the adoption of the general provision proposed above, on the basis of the latter provision. For example, according to the current initiatives related to intelligent transport systems the Commission will bear specific initial responsibility in the definition of measures, standardisation initiatives, procedures and best practices. In carrying out these tasks, the PbD should be a guiding principle.

44. The EDPS further notes that the privacy by design principle is also of specific importance in the area of freedom, security and justice, in particular in relation to the goals of the Information Management Strategy, as foreseen in the Stockholm Programme[22]. In his opinion relating to the Stockholm Programme the EDPS emphasized that the architecture for information exchange should be based on 'privacy by design'[23]: "This means, more concretely, that information systems which are designed for purposes of public security should always be built in accordance with the principle of 'privacy by design'".

45. The Article 29 Working Party's Opinion on the future of privacy[24] insists in even more precise terms that in the area of freedom, security and justice - where public authorities are the main actors and where measures increasing surveillance directly impact on the fundamental rights to privacy and data protection - requirements of privacy by design should be made compulsory. By introducing these requirements in information systems, governments would also stimulate privacy by design in their capacities as launching customers.

PbD as a guiding principle in Europe's Digital Agenda

46. Information and communication technologies are increasingly complex and entail greater privacy and data protection risks. In general, digitised information, which is easier to access, copy and transmit is exposed to much higher risks than paper based information. As we move towards networks of interconnected objects, the risks will increase. The greater privacy/data protection risks are, the greater will be the demand for enhanced data protection/privacy safeguards. Therefore, the justifications for the need to implement PbD are more compelling in the ICT sector. In addition, as discussed above, individuals' trust in ICT is fundamental if citizens are to embrace these new services, and privacy and data protection are key elements of such trust.

47. The above underlines that a strategy for the development of ICT must confirm the need for them to be designed with an inherent element of privacy and data protection, i.e.

---

[22] The Stockholm Programme - An open and secure Europe serving and protecting the citizen, approved by the European Council in December 2009.

[23] Opinion of 10 July 2009 on the Communication from the Commission to the European Parliament and the Council on an Area of freedom, security and justice serving the citizen, OJ C 276, p. 8, pt 60.

[24] Article 29 Working Party Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1st December 2009.

taking into consideration the principle of privacy by design.

48. Therefore, the European Digital Agenda should explicitly endorse the principle of privacy by design as a necessary element to ensure citizen trust in ICT and online services. It should recognise that privacy and trust go hand in hand, and that privacy by design should be a guiding factor in the development of a trustworthy ICT sector.

PbD as a principle in other EU-initiatives

49. The Commission should have privacy by design as a guiding principle in implementing policies, activities and initiatives in specific ICT sectors, including eHealth, eProcurement, eSocial Security, eLearning, etc. Many of these initiatives will be action items in the European Digital Agenda.

50. This means, for example, that initiatives to ensure that government applications are more efficient and modern so that individuals can interact with administrations, should include the need for them to be designed and operated in accordance with the principle of privacy by design. The same applies to Commission policies and activities that cater for a faster Internet, digital content, or overall encouragement of fixed and wireless communications and data transmission.

51. The above also includes areas where the Commission is responsible for the large scale IT systems, like SIS and VIS, as well as for those cases whereby the Commission's responsibility is limited to the development and maintenance of the common infrastructure of such a system, such as the European Criminal Records Information System (ECRIS).

52. How exactly the PbD principle will be developed will depend on each particular sector and situation. For example, when Commission initiatives are accompanied by legislative proposals on a specific ICT sector, in many cases it will be appropriate to include an explicit reference to the notion of PbD applicable to the design of the particular ICT application/system. If action plans for a specific area are designed, they should systematically ensure the application of the legal framework and more specifically guarantee that the relevant ICT technology is built with privacy by design in mind.

53. As far as research is concerned, the Seventh Framework Programme and the following ones should be used as a tool to support projects that aim at analysing standards, ICT technologies and architecture that better serve privacy and more particularly the principle of privacy by design. In addition, PbD should also be a necessary element to be considered in broader ICT projects that aim at processing personal data of individuals.

Areas of specific concern

54. In some cases, because of the particular risks for individuals' privacy and data protection or due to other factors (industry resistance to provide PbD products, consumer demand, etc) it may be necessary to define more explicit and specific privacy by design measures that must be incorporated into a given type of information and communication product/technology, either or not in legislative instruments.

55. The EDPS has identified various areas (RFID, social networking and browser applications) that deserve, in his opinion, at this stage careful consideration by the

Commission and the more hands-on intervention advocated above. These three areas are discussed further below.

VI. RADIO FREQUENCY IDENTIFICATION-RFID

56. RFID tags can be integrated into objects, animals and people. They can be used to collect and store personal data such as medical records, to trace people's movements or to profile their behaviour for different purposes. This can be done without the individual being aware of it[25].

57. Effective guarantees regarding data protection, privacy and all associated ethical dimensions are crucial for public trust in RFID and a future Internet of Things. Only then can the technology deliver its numerous economic and societal benefits.

VI.1. The gaps of the applicable data protection legal framework

58. The Data Protection Directive and the ePrivacy Directive apply to the collection of data carried out through RFID applications[26]. They require, among others, that adequate privacy safeguards are put in place to operate RFID applications[27].

59. However, this legal framework does not fully address all the data protection and privacy concerns raised by this technology. This is because the Directives are not sufficiently detailed as to the type of safeguards that should be implemented in RFID applications. The existing rules need to be complemented with additional ones imposing specific safeguards, particularly making mandatory to embed technical solutions (privacy by design) in RFID technology. This is true for tags that store personal information, which should have kill commands and the use of cryptography in tags storing certain types of personal information.

---

[25] RFID stands for Radio Frequency Identification. The main components of Radio Frequency identification technology *or* infrastructure are a *tag* (i.e. a microchip), a reader and application linked to the tags and readers through middleware and processing the data produced. The tag consists of an electronic circuit that stores data and an antenna which communicates the data via radio waves. The reader possesses an antenna and a demodulator which translates the incoming analogue information from the radio link into digital data. The information can then be sent through networks to databases and servers in order to be processed by a computer.

[26] The ePrivacy Directive refers to RFID in Article 3 "*This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices*" This is complemented by Recital 56) "*Technological progress allows the development of new applications based on devices for data collection and identification, which could be contactless devices using radio frequencies. For example, Radio Frequency Identification Devices (RFIDs) use radio frequencies to capture data from uniquely identified tags which can then be transferred over existing communications networks. The wide use of such technologies can bring considerable economic and social benefit and thus make a powerful contribution to the internal market, if their use is acceptable to citizens. To achieve this aim, it is necessary to ensure that all fundamental rights of individuals, including the right to privacy and data protection, are safeguarded. When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC (Directive on privacy and electronic communications), including those on security, traffic and location data and on confidentiality, should apply*".

[27] For example, Article 17 of the data protection Directive imposes an obligation to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or unauthorized disclosure.

VI.2. Self-regulation as a first step

60. In March 2007, the Commission adopted a Communication[28] recognising, among others, the need for detailed guidance on practical implementation of RFID and the desirability of adopting design criteria to avoid risks to privacy and security.

61. To achieve these goals, in May 2009, the Commission adopted a recommendation on the implementation of privacy and data protection principles in RFID applications[29]. In retail RFID applications, it requires tag deactivation at the point of sale unless individuals have consented. This applies unless a privacy and data protection impact assessment demonstrates that tags do not represent a likely threat to privacy or the protection of personal data, in which case they would remain operational after the point of sale unless the individuals opt-out, free of charge.

62. The EDPS agrees with the Commission's approach to use self-regulatory instruments. However, as further described below, it is conceivable that self-regulation will not deliver the expected results; therefore he calls upon the Commission to be ready to adopt alternative measures.

VI.3. Areas of concern and possible additional measures if self-regulation fails

63. The EDPS is concerned that organizations operating RFID applications in the retail sector may overlook the possibility for RFID tags to be monitored by unwanted third parties. Such monitoring might reveal personal data stored in the tag (if any), but might also enable a third party to follow or recognize a person through time by simply using the unique identifiers contained in one or several tags carried by the individual, in an environment that may even be outside of the operational perimeter of the RFID application. He is further concerned that operators of RFID applications may be tempted to unduly rely on the exception, and thus, leave the tag operational after the point of sale.

64. If the above occurs, it may be too late to mitigate the risks to individuals' data protection and privacy, which may have already been affected. Further, given the nature of self-regulation, national enforcement authorities may have a weaker position when requiring organizations operating RFID applications to apply specific privacy by design measures.

65. In the light of the above, the EDPS calls upon the Commission to be ready to propose legislative instruments regulating the main issues of RFID usage in case the effective implementation of the existing legal framework fails. The Commission's assessment should not be unduly postponed; postponing would put individuals at risk and it would also be counterproductive for industry as the legal uncertainties are too high and entrenched problems are likely to be more difficult and expensive to correct.

66. Within the measures that may need to be proposed, the EDPS recommends providing for the opt-in principle at the point of sale pursuant to which all RFID tags attached to consumer products would be deactivated by default at the point of sale. It may not be necessary or appropriate for the Commission to specify the concrete technology to be

[28] Communication from the Commission of 15.3.2007 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 final.

[29] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (C (2009) 3200 final).

used. Instead, Union law must establish he legal obligation to obtain opt-in consent, leaving room for operators to decide the ways to meet the requirement.

VI.4. Further issues to consider: Governance of the Internet of things

67. Information produced by RFID tags - for example, product information - may eventually be interconnected into a global network of communication infrastructure. This is usually referred to as the 'Internet of things'. The data protection/privacy questions arise because real world objects may be identified by RFID tags that in addition to product information may include personal data.

68. There are many open questions about who will manage the storage of information related to tagged items. How will it be organized? Who will have access to it? In June 2009, the Commission adopted a Communication on the Internet of Things[30] which has explicitly identified the potential data protection and privacy problems of this phenomenon.

69. The EDPS would like to stress some of the issues raised by the Communication which, in his view, deserve close attention as the Internet of Things develops. First, the need for a decentralized architecture may facilitate accountability and enforceability of the EU legal framework. Second, the individuals' right to not be tracked should be preserved, to the extent possible. In other words, there should be very limited cases where individuals' are tracked through RFID tags without their consent. Such consent should be explicit. This is usually referred to as the "silence of chips" and the right to be left alone. Finally, in designing the Internet of Things, the principle of privacy by design should be a guiding principle. For example, this would require that concrete RFID applications which have inbuilt mechanisms to give control to users are designed with privacy by default settings.

70. The EDPS expects to be consulted as the Commission puts in place the actions envisaged in the Communication, particularly the drafting of the Communication on privacy and trust in the ubiquitous information society.

VII. SOCIAL NETWORKS AND THE NEED FOR DEFAULT PRIVACY SETTINGS

71. Social networks are the "flavour of the month". They appear to have surpassed email in popularity. They connect people with others who share similar interests and/or activities. People can have their profiles online and share media files such as videos, photos, music as well as their career profiles.

72. Young people have rapidly adopted social networking and this trend is continuing. The average age of Internet users in Europe has decreased in the past few years: 9-10 year olds now connect several times a week; 12-14 year olds go online daily, often for one to three hours.

[30] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Internet of Things- An action plan for Europe, 18.6.2009, COM (2009) 278 final.

VII.1. Social networks and the applicable legal framework for data protection and privacy

73. The development of social networks has enabled users to upload onto the Internet information about themselves and third parties. In doing so, according to Article 29 Working Party[31], Internet users act as data controllers *ex* Article 2(d) of the Data protection Directive for the data that they upload[32]. However, in most cases such processing falls within the household exception *ex* Article 3.2. of the Directive. At the same time, social networking services are considered data controllers insofar as they provide the means for the processing of user data and provide all the basic services related to user management (e.g. registration and deletion of accounts).

74. In legal terms this means that Internet users and social networking services share joint responsibility for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Directive, albeit to different degrees and with different sets of obligations.

75. Accordingly, users should know and understand that by processing their personal information and that of others, they fall under the provisions of the EU legislation on data protection that requires, among other things, obtaining the informed consent of those whose information is uploaded and granting those concerned with the right of rectification, object, etc. Similarly, social networking services must, among other things, implement appropriate technical and organisational measures to prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data. This in turn means that social networking services should ensure privacy-friendly default settings, including settings that restrict profile access to the user's own, self-selected contacts. Settings should also require user's affirmative consent before any profile becomes accessible to other third parties, and restricted access profiles should not be discoverable by internal search engines.

76. Unfortunately, there is a gap between legal requirements and actual compliance. Whereas legally speaking Internet users are considered data controllers and are bound by the EU data protection and privacy legal framework, in reality, they are often unaware of this role. Generally speaking they have a poor understanding that they are processing personal data and that there are privacy and data protection risks involved in publishing such information. Young people in particular post content online underestimating the consequences for them and others, for example, in the context of subsequent enrolment in educational institutions or applications for jobs.

77. At the same time, social network providers often preselect default settings based on opt-outs, thus facilitating the disclosure of personal information. Some enable profiles to be available to common search engines by default. This raises questions as to whether individuals have actually consented to disclosure, as well as whether social networks have complied with Article 17 of the Directive (described above) requiring them to implement appropriate technical and organisational measures to prevent unauthorised processing.

[31] See Article 29 Working Party Opinion163, 5/2009 on online social networking, adopted on 12 June 2009 .

[32] 'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community law.

VII.2. Risks generated by social networks and suggested actions to address them

78. The above results in an increased risk to individual's privacy and data protection. It exposes Internet users and those whose data has been uploaded to blatant violations of their privacy and data protection.

79. Against this background, the question that the Commission should address is what should and could be done to address this situation. This Opinion does not provide a comprehensive answer to the question, but instead puts forward a number of suggestions for further consideration.

Investing in Internet's users education

80. The first suggestion is to invest in user education. In this regard, the EU institutions and national authorities should invest in educating and raising awareness of the threats posed by social networking websites. For example, DG Information Society has been running the Safer Internet Programme, which aims at empowering and protecting children and young people by, for instance, awareness raising activities[33]. Recently the EU institutions launched the 'Think before you post' campaign to raise awareness of the risks of sharing personal information with strangers.

81. The EDPS encourages the Commission to continue to support this type of activity. However, social network providers themselves should also play an active role, as they have a legal and social responsibility to educate users in how to use their services in a safe and privacy-friendly manner.

82. As described above, when posting information on social networks, the information may be made available by default in a number of different ways. For example, information may be available to the public in general, including search engines, which may index it and thus provide direct links to it. On the other hand, information may be limited to "selected friends" or may be kept completely private. Obviously, the profile permissions and the terminology used vary from site to site.

83. However, as outlined above, very few users of social networking services know how to control access to the information they post, never mind how to change the default privacy settings. Privacy settings usually remain unchanged because users are unaware of the implications of not changing them or do not know how to do it. More often than not therefore, not changing the privacy settings does not mean that individuals have made an informed decision to accept sharing information. In this context, it is particularly important that third parties such as search engines do not link to individual profiles, on the assumption that users have consented by default (by not changing the privacy settings) to make the information available without restrictions.

84. Whilst user education may help to address this situation, it will not work on its own. As recommended by the Article 29 Working Party in its Opinion on social networks, social network providers should offer privacy-friendly, free-of-charge default privacy settings. This would make users more aware of their actions, and enable them to make better choices as to whether they want to share information and with whom.

33 Information about such program is available at:
http://ec.europa.eu/information_society/activities/sip/index_en.htm

Role for self-regulation

85. The Commission has entered into an agreement with twenty social network providers known as the "Safer Social Networking Principles for the EU"[34]. The aim of the agreement is to improve the safety of minors when using social networking sites in Europe. Such principles include many of the requirements derived from the application of the data protection legal framework described above. They include, for example, the requirement to empower users through tools and technology, to ensure that they can control the use and dissemination of their personal information. It also includes the need to provide privacy settings by default.

86. Early January 2010, the Commission made available the findings of a report evaluating the implementation of the principles[35]. The EDPS is concerned that this report shows that while some steps have been taken, many others have not. For example, the report found problems regarding the communication of the safety measures and tools available on the sites. It also found that less than half of the signatories of the agreement restrict access to the profiles of minors to only their friends.

Need for mandatory privacy by default settings

87. In this context, the key question is whether additional policy measures are necessary to ensure that social networks set up their services with privacy by default settings. This issue was raised by the former Information Society Commissioner Viviane Reding, who pointed out that legislation may be necessary.[36] Along the same lines, the European Economic and Social Committee stated that alongside self-regulation minimum protection standards should be imposed by law[37].

88. As noted above, the obligation for social network providers to implement by default privacy settings can be deduced indirectly from Article 17 of the Data protection Directive[38] which obliges data controllers to take appropriate technical and organisational measures (*'both at the time of the design of the processing system and at the time of the processing itself'*) to maintain security and prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data.

89. However, this article is far too general and lacks specificity, also in this context. It does not state clearly what is meant by appropriate technical and organisational measures in the context of social networks. Thus, the current situation is one of legal uncertainty, which causes problems for both regulators and individuals whose privacy and personal data are not fully protected.

90. In light of the above, the EDPS urges the Commission to prepare legislation which would include, at a minimum, an overarching obligation requiring mandatory privacy settings, coupled with more precise requirements:

---

[34] The principles are available at:
http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
[35] Report on the assessment of the implementation of the Safer Social Network Principles for the EU, available at:
http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf.

[36] Viviane Reding, Member of the European Commission responsible for Information Society and Media Think before you post! How to make social networking sites safer for children and teenagers? Safer Internet Day Strasbourg, 9 February 2010.
[37] Opinion of the European Economic and Social Committee on the Impact of social network sites on citizens/consumers, 4, November 2009.
[38] Also expanded in point 33 of this document.

a) providing settings that restrict access to user profiles to the user's own, self-selected contacts. Settings should also require user's affirmative consent before any profile is accessible to third parties;
b) providing that restricted access profiles should not be discoverable by internal/external search engines.

91. In addition to providing for mandatory privacy by default settings, a question remains as to whether additional, specific data protection and other measures (for example, regarding protection of minors) may also be appropriate. This raises the broader issue of whether it would be suitable to create a specific framework for these types of services that, in addition to providing for mandatory privacy settings, would regulate other aspects. he EDPS asks the Commission to take this issue into consideration.

VIII. PRIVACY BY DEFAULT BROWSER SETTINGS TO GUARANTEE INFORMED CONSENT TO RECEIVE ADS

92. Ad network providers use cookies and other devices to monitor the behaviour of individual users when they surf the Internet in order to catalogue their interests and build profiles. This information is then used to send them targeted advertisements[39].

VIII.1. Remaining challenges and risks under the current data protection/privacy legal framework

93. This processing is covered by the Data Protection Directive (when personal data is concerned) and also by Article 5.3 of the ePrivacy Directive. This article specifically requires that the user is informed and given the opportunity to react by way of consenting to or rejecting the storage of devices such as cookies etc on his computer or other device [40] .

94. To the present, ad network providers have relied on browser settings and privacy policies to inform users and enable them to consent or reject cookies. They have explained in publishers privacy policies how to opt-out from receiving cookies altogether or to accept them on a case-by-case basis. In doing so, they intended to comply with their obligation to offer users the right to refuse cookies.

95. Whereas theoretically this method (via the browser) could indeed effectively provide meaningful informed consent, the reality is very different. In general, users lack the basic understanding of the collection of any data, much less from third parties, of the value of such data, its uses, how the technology works and more particularly how and where to opt-out. The steps that users must take to opt-out seem not only complicated but also excessive (first he must set his browser to accept cookies, then exercise the opt-out option).

[39] Tracking cookies are small text files containing a unique identifier. Typically, ad network providers (as well as Web site operators or publishers) place cookies on the visitors' hard disk, in particular in the browser of Internet users, when the users first access Web sites serving ads that are part of their network. The cookie will enable the ad network provider to recognize a former visitor who returns to that Web site or visits any website which is a partner of the advertising network. Such repeated visits will enable the ad network provider to build a profile of the visitor.

[40] Article 5(3) of the ePrivacy Directive was recently amended to reinforce the protection against interception of users' communications through the use of - for example - spyware and cookies stored on a user's computer or other device. Under the new Directive users should be offered better information and easier ways to control whether they want cookies stored in their terminal equipment.

96. As a result, in practice very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertisement, but rather because they do not realise that by not using the opt out, they are in fact accepting.

97. Therefore, while legally speaking, Article 5(3) of the ePrivacy Directive provides for effective legal protection, in practice, Internet users are deemed to consent to be monitored for the purposes of sending behavioural advertisement when in fact, in many, if not most cases, they are fully unaware that the monitoring takes place.

98. The Article 29 Working Party is preparing an opinion that aims to clarify the legal requirements to engage in behavioural advertisement, which is welcome. However, interpretation may not, in itself, be sufficient to solve this situation and it may be necessary for the European Union to take additional actions.

VIII.2. Need for further action, notably providing for mandatory privacy by default settings

99. As described above, web browsers commonly allow a level of control over certain kinds of cookies. Currently, the default settings of most web browsers are accepting all cookies. In other words, by default, the browsers are set to accept all cookies, independently of the purpose of the cookie. Only if the user changes the settings of his/her browser application to deny cookies, which as described above, very few users do, he/she will not receive cookies. Furthermore, there is no privacy wizard on the first install or update of browser applications.

100. A way to mitigate the above problem would be if browsers would be provided with by default privacy settings. In other words, if they would be provided with the setting of 'not acceptance of third party cookies'. To complement this and to make it more effective, the browsers should require users to go through a privacy wizard when they first install or update the browser. There is a need for more granularity and clear information on the types of cookies and the usefulness of some of them. Users willing to be monitored for the purposes of receiving advertisement will be duly informed and they would need to change the browser settings. This would give them an enhanced control over their personal data and privacy. This would be, in the EDPS' view, an effective way to respect and preserve users' consent[41].

101. Taking into account, on the one hand, the widespread nature of the problem, in other words, the number of Internet users that are currently monitored on the basis of a consent that is illusory and, on the other, the scale of interest at stake, the need for additional safeguards becomes more acute. The implementation of the PbD principle in web browser applications could make a dramatic difference towards giving individuals control over the data collection practices used for advertising purposes.

102. For these reasons, the EDPS urges the Commission to consider legislative measures requiring mandatory privacy by default settings in browsers and the provision of the relevant information.

[41] At the same time, the EDPS is aware that this would not completely solve the problem insofar as there are cookies which can not be controlled through the browser, such as the case with the so-called flash cookies. For this, it would be necessary for browser developers to integrate flash controls into their cookie controls by default in the releases of new browsers.

IX. OTHER PRINCIPLES AIMING AT PROTECTING INDIVIDUALS' PRIVACY/DATA PROTECTION

103. While the PbD principle has a great potential to improve the protection of individuals' personal data and privacy, the design and implementation in law of complementary principles to ensure consumer trust in ICT are necessary. Against this background, the EDPS addresses the accountability principle and the completion of a mandatory security breach framework applicable across sectors.

IX.1. The accountability principle to ensure compliance with the principle of privacy by design

104. The Article 29 Working Party paper entitled "Future of Privacy"[42] recommended including the accountability principle into the Data Protection Directive. This principle, which is recognised in some multinational data protection instruments[43], requires organizations to implement processes to comply with existing laws and to set up methods of assessing and demonstrating compliance with the law and other binding instruments.

105. The EDPS fully supports the Article 29 Working Party recommendation. He considers that this principle will be highly relevant to foster the effective application of data protection principles and obligations. Accountability will require data controllers to demonstrate that they have put in place the mechanism necessary to comply with applicable data protection legislation. This is likely to contribute to the effective implementation of privacy by design in ICT technologies as a particularly well-suited element to show accountability.

106. To measure and demonstrate accountability data controllers could use internal procedures and third parties who may perform audits or other types of checks and verifications, which as a result, may award seals or awards. In this context, the EDPS urges the Commission to consider whether, in addition to a general accountability principle, it may be helpful to require by law specific accountability measures such as the need to produce privacy and data protection impact assessments and under which circumstances.

IX.2. Security breach: completing the legal framework

107. Last year's amendments to the ePrivacy Directive introduced a requirement to notify data breaches to affected individuals and also to the relevant authorities. A data breach is broadly defined as any breach leading to the destruction, loss, disclosure etc of personal data transmitted, stored or otherwise processed in connection with the service. Notification to individuals will be required if the data breach is likely to adversely affect their personal data or privacy. This may be the case where the breach could lead to identity theft or significant humiliation or reputational damage. Notification to the relevant authorities will be required for every data breach, regardless of whether there is a risk to individuals.

---

[42] Article 29 Working Party Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1st December 2009.

[43] 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Madrid Privacy Declaration on Global Privacy Standards for a Global World, of 3 November 2009.

Applying security breach obligations across sectors

108. Unfortunately this obligation applies only to providers of publicly available electronic communications services, such as telephone companies, Internet Access Providers, Webmail providers, etc. The EDPS urges the Commission to put forward proposals on security breach applying across sectors. As to the content of such framework, the EDPS considers that the security breach legal framework adopted in the ePrivacy Directive strikes an appropriate balance between the protection of individuals' rights, including their rights to personal data and privacy, and the obligations imposed on covered entities. At the same time, this is a framework with real "teeth," as it is backed by meaningful enforcement provisions, which provide authorities with sufficient powers of investigation and sanction in the event of non-compliance.

109. Accordingly, the EDPS urges the Commission to adopt a legislative proposal applying this framework across sectors, if necessary with the appropriate adjustments. In addition this would ensure that the same standards and procedures are applied across sectors.

Completing the legal framework embedded in the ePrivacy Directive through comitology

110. The revised ePrivacy Directive empowers the Commission to adopt technical implementing measures, i.e. detailed measures on security breach notification, through a comitology procedure.[44] This empowerment is justified in order to ensure consistent implementation and application of the security breach legal framework. Consistent implementation works towards ensuring that individuals across the Community enjoy an equally high level of protection and that covered entities are not burdened with diverging notification requirements.

111. The ePrivacy Directive was adopted in November 2009. There does not appear to be any reason justifying postponing the starting of the work towards adopting the technical implementing measures. The EDPS organised two seminars which aimed at sharing and gathering experience on data breach notification. He would be happy to share the results of this exercise and is looking forward to working with the Commission and other stakeholders in fine-tuning the overall data breach legal framework.

112. The EDPS urges the Commission to take the necessary steps, within a short timeframe. Before adopting technical implementing measures, the Commission must engage in a broad consultation, in which ENISA, the EDPS and Article 29 Working Party must be consulted. Furthermore, the consultation must also include other "relevant stakeholders", particularly in order to inform of the best available technical and economic means of implementation.

[44] Comitology involves the adoption of technical implementing measures through a committee of Member State representatives chaired by the Commission. For the ePrivacy Directive, the so called regulatory procedure with scrutiny applies, meaning that the European Parliament, as well as Council, can oppose measures proposed by the Commission. See further http://europa.eu/scadplus/glossary/comitology_en.htm.

X. CONCLUSIONS

113. Trust, or rather its absence, has been identified as a core issue in the emergence and successful deployment of information and communications technologies. If people do not trust ICT, these technologies are likely to fail. Trust in ICT depends on different factors; ensuring that such technologies do not erode individuals' fundamental rights to privacy and to the protection of personal data is a key one.

114. In order to further strengthen the data protection/privacy legal framework, the principles of which remain completely valid in the information society, the EDPS proposes the Commission to embed Privacy by Design on different levels of law and policy making.

115. He recommends the Commission to follow four courses of action:
    a) Propose to include a general provision on Privacy by Design in the legal framework for data protection. This provision should be technology neutral and compliance should be mandatory at different stages;
    b) Elaborate this general provision in specific provisions, when specific legal instruments in different sectors are proposed. These specific provisions could already now be included in legal instruments; on the basis of Article 17 of the Data Protection Directive (and other existing law);
    c) Include PbD as a guiding principle in Europe's Digital Agenda;
    d) Introduce PbD as a principle in other EU-initiatives (mainly non legislative).

116. In three designated ICT areas, the EDPS recommends the Commission to evaluate the need to put forward proposals implementing the principle of Privacy by Design in specific ways:
    a) In relation to RFID, propose legislative measures regulating the main issues of RFID usage in case the effective implementation of the existing legal framework through self-regulation fails. In particular, provide for the opt-in principle at the point of sale pursuant to which all RFID tags attached to consumer products would be deactivated by default at the point of sale;
    b) In relation to social networks, prepare legislation which would include, as a minimum, an overarching obligation requiring mandatory privacy settings, coupled with more precise requirements, on the restriction of access to user profiles to the user's own, self-selected contacts, and providing that restricted access profiles should not be discoverable by internal/external search engines;
    c) In relation to targeted advertising, consider legislation mandating browser settings to reject third party cookies by default and require users to go through a privacy wizard when they first install or update the browser.

117. Finally, the EDPS suggests the Commission to:

    a) Consider implementing the accountability principle in the existing data protection Directive, and
    b) Develop a framework of rules and procedures to implement the security breach notification provisions of the e-Privacy Directive, and extend them to apply generally to all data controllers.

Done in Brussels, 18 March 2010

(**signed**)
Peter HUSTINX
European Data Protection Supervisor