ISSN 1725-2423

Official Journal of the European Union

C 280

English edition

Volume 53

16 October 2010

Information and Notices

Notice No | Contents | Page

EN

Price: EUR 3

[1] Text with EEA relevance, except for products falling under Annex I to the Treaty

(Continued overleaf)

EN

(1) Text with EEA relevance, except for products falling under Annex I to the Treaty

(2) Text with EEA relevance

(Continued on inside back cover)

I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

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

(2010/C 280/01)

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 [1],

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 [2],

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 [3], 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 [4].

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 [5]. 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 [6].

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 201, 31.7.2002, p. 37.
[3] OJ L 8, 12.1.2001, p. 1.

[4] Answers to European Parliament Questionnaire for Commissioner Neelie Kroes in the context of the EP hearings that preceded the Commissioner's designation.
[5] 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.
[6] 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. 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 ([1]). 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 ([2]).

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, eGovernment 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 ([3]) 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 — Towards an open, green and competitive knowledge society' ([4]). The

([1]) 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.

([2]) 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, 23.4.2008, 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, 18.7.2008, 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.

([3]) Europe's Digital Competitiveness Report—Main achievements of the i2010 strategy 2005-2009 (SEC(2009) 1060).

([4]) Council Conclusions 'Post i2010 Strategy — Towards an open, Green and Competitive Knowledge Society' (17107/09), adopted on 18.12.2009.

European Parliament has just adopted a report intended to provide guidance to the Commission in defining a digital agenda ([1]).

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 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 ([2]). 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

([1]) Report on defining a new Digital Agenda for Europe: from i2010 to digital.eu (2009/2225 (INI)), adopted on 18.3.2010.

([2]) 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.

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.

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 ([1]). 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.

([1]) 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

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 ([2]).

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. ([3]).

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, 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

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

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

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 ([1]), Directive 2002/58/EC ([2]) and the jurisprudence of the European Court of Human Rights ([3]) 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 Directive deals specifically with the protection of privacy in the electronic communication sector ([4]).

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 organisation measures to prevent unlawful data processing ([5]). 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 standardisation.

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 ([6]).

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

([1]) Directive 95/46/EC of the European Parliament and of the Council (further: Data Protection Directive).

([2]) Directive 2002/58/EC of the European Parliament and of the Council (further: ePrivacy Directive).

([3]) 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.

([4]) 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 Rights became binding when the Lisbon Treaty entered into force.

([5]) Article 17 reads as follows: 'Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss and against unauthorised 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 organisational 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 unauthorised processing'.

([6]) The Commission has announced plans to update Directive 1999/5/EC towards the end of 2010.

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 [1]. 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.

37. In the EDPS' view, which is shared with the Article 29 Working Party [2], 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 [3].

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,

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

[2] 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 1 December 2009.

[3] '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.

manufacturers, data controllers and DPAs, to interpret the meaning of the principle in 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 [1]. In his opinion relating to the Stockholm Programme the EDPS emphasised that the architecture for information exchange should be based on 'privacy by design' [2]: '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 [3] 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. 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.

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

[2] 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, 17.11.2009, p. 8, point. 60).

[3] 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.

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.

V. **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 [1].

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.

V.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 [2]. They require, among others, that adequate privacy safeguards are put in place to operate RFID applications [3].

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

[1] 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.

[2] 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'.

[3] For example, Article 17 of the Data Protection Directive imposes an obligation to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure.

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.

V.2. **Self-regulation as a first step**

60. In March 2007, the Commission adopted a Communication ([1]) 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 ([2]). 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.

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

63. The EDPS is concerned that organisations 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 organisations 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 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.

V.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 organised? Who will have access to it? In June 2009, the Commission adopted a Communication on the Internet of Things ([3]) which has explicitly identified the potential data protection and privacy problems of this phenomenon.

([1]) 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.

([2]) 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).

([3]) 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.

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 decentralised 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.

VI. **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.

VI.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 ([1]), Internet users act as data controllers ex Article 2(d) of the Data Protection Directive for the data that they upload ([2]). 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.

([1]) See Article 29 Working Party Opinion 163, 5/2009 on online social networking, adopted on 12 June 2009.

([2]) '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.

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.

VI.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, Information Society DG has been running the Safer Internet Programme, which aims at empowering and protecting children and young people by, for instance, awareness raising activities ([1]). 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.

Role for self-regulation

85. The Commission has entered into an agreement with 20 social network providers known as the 'Safer Social Networking Principles for the EU' ([2]). 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 ([3]). The EDPS is concerned that this report shows that while some steps have been taken, many others have not. For example, the report found

([1]) Information about such program is available at: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) The principles are available at: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) 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

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 ([1]). Along the same lines, the European Economic and Social Committee stated that alongside self-regulation minimum protection standards should be imposed by law ([2]).

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 ([3]) 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:

(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. The EDPS asks the Commission to take this issue into consideration.

VII. **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 ([4]).

VII.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 ([5]).

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

([1]) 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.

([2]) Opinion of the European Economic and Social Committee on the Impact of social network sites on citizens/consumers, 4 November 2009.

([3]) Also expanded in point 33 of this document.

([4]) Tracking cookies are small text files containing a unique identifier. Typically, ad network providers (as well as website operators or publishers) place cookies on the visitors' hard disk, in particular in the browser of Internet users, when the users first access website serving ads that are part of their network. The cookie will enable the ad network provider to recognise a former visitor who returns to that website 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.

([5]) 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.

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).

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.

VII.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 [1].

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.

VIII. **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.

VIII.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' [2] recommended including the accountability principle into the Data Protection Directive. This principle,

[1] At the same time, the EDPS is aware that this would not completely solve the problem insofar as there are cookies which cannot 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.

[2] 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.

which is recognised in some multinational data protection instruments [1]), requires organisations 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.

VIII.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.

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 [2]). 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 time-frame. 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.

([1]) 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.

([2]) 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

IX. **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 at Brussels, 18 March 2010.

Peter HUSTINX

European Data Protection Supervisor

Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)

(2010/C 280/02)

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 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, and in particular its Article 17,

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 3 December 2008 the Commission adopted a Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) (hereinafter 'the Proposal') ([1]). The Proposal aims to recast Directive 2002/96/EC on waste electrical and electronic equipment (WEEE) adopted on 27 January 2003 (hereinafter 'the Directive') ([2]) without changing either the drivers or the rationale for collecting and recycling WEEE.

2. The EDPS has not been consulted as required by Article 28(2) of Regulation (EC) No 45/2001 ([3]). Acting on his own initiative, the EDPS has therefore adopted the current opinion based on Article 41(2) of the same Regulation. The EDPS recommends that a reference to this opinion is included in the preamble of the Proposal.

3. The EDPS is aware that this advice comes at a late stage in the legislative process but nevertheless considers it appropriate and useful to issue this opinion, since the Proposal raises significant data protection issues not addressed in the text. This opinion is not meant to modify the main and predominant purpose and content of the Proposal, whose 'centre of gravity' ([4]) remains in the protection of the environment, but only to bring an additional dimension which is becoming increasingly important to our information society ([5]).

4. The EDPS, also aware of the limited scope of the recasting procedure, nevertheless urges the legislator to take these recommendations into account in accordance with Article 8 of the Interinstitutional Agreement on the recasting procedure (which provides for the possibility of amending unchanged provisions) ([6]).

II. CONTEXT AND BACKGROUND OF THE PROPOSAL AND ITS RELEVANCE TO DATA PROTECTION

5. The purpose of the Proposal is to update the existing Directive relating to the disposal, reuse and recycling of WEEE. Technical, legal and administrative problems in the first years of implementation of the Directive have led to the Proposal, as was foreseen under Article 17(5) of the Directive.

6. Electric and electronic equipment (EEE) is a wide product group that includes a diverse set of media capable to store personal data — such as IT and telecommunications equipment (e.g. personal computers, laptops, electronic communication terminals) — characterised in the present techno-economic context by increasingly fast innovation cycles and, due to technological convergence, by the availability of multi-purpose devices. Developments in electronic storage media are accelerating rapidly, particularly in relation to storage capacity and size, and therefore market forces cause the turnover of EEE (containing large amounts of, often sensitive, personal data) to accelerate similarly. The results being not only that the WEEE 'is considered the fastest growing waste stream in

([1]) COM(2008) 810 final.
([2]) OJ L 37, 13.2.2003, p. 24.
([3]) 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 (OJ L 8, 12.1.2001, p. 1).
([4]) See ECJ, 23.2.1999, C-42/97 European Parliament v Council of the European Union, [1999] ECR I-869, par. 43.
([5]) See also, inter alia, ECJ, 30.1.2001, C-36/98 Spain v Council, [2001] ECR I-779, par. 59: 'If examination of a Community measure reveals that it pursues a twofold purpose or that it has a twofold component and if one of these is identifiable as the main or predominant purpose or component, whereas the other is merely incidental, the act must be based on a single legal basis, namely that required by the main or predominant purpose or component'.
([6]) Interinstitutional Agreement of 28 November 2001 on a more structured use of the recasting technique for legal acts (OJ C 77, 28.3.2002, p. 1).

the EU' ([7]), but also, in the case of inappropriate disposal, that there is an obvious increased risk of loss and dispersion of personal data stored within this type of EEE.

7. For a long time the European Union's policies on the environment and sustainable development have been aimed at reducing waste of natural resources and introducing measures to prevent pollution.

8. The disposal, reuse and recycling of WEEE are included within this framework. These measures seek to prevent the disposal of electrical and electronic equipment along with mixed waste, placing an obligation on producers to provide disposal in the manner prescribed by the Directive.

9. In particular, among the various measures envisaged by the Directive, it is worth highlighting those designed to *reuse* (i.e. any operation by which WEEE or components thereof are used for the same purpose for which they were conceived, including the continued use of the equipment or components thereof which are returned to collection points, distributors, recyclers or manufacturers), *recycle* (i.e. the reprocessing in a production process of the waste materials for the original purpose or for other purposes) and find other forms of recovery of WEEE so as to reduce the disposal of waste (see Articles 1 and 3(d) and (e) of the Directive).

10. These operations, in particular the reuse and recycling of the WEEE, especially IT and telecommunications equipment, may present a risk, greater than in the past, that those collecting the WEEE or selling and purchasing the used or recycled devices might become aware of any personal data stored within. Such data can often be sensitive or refer to large numbers of individuals.

11. For all these reasons, the EDPS considers it urgent for all stakeholders (users and producers of EEE) to be made aware of the risks to personal data, especially in the final stage of the EEE life-cycle. At this stage, although the EEE are economically less valuable, they are likely to contain a large amount of personal data and therefore likely to have a high 'intrinsic' value for the data subject and/or others.

([7]) See Commission Staff working paper accompanying the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) (recast). Impact Assessment, 3.12.2008 (COM(2008) 810 final) SEC(2008) 2933, p. 17.

III. ANALYSIS OF THE PROPOSAL

III.1. Applicability of Directive 95/46/EC

12. The EDPS has no observations on the general objective of the Proposal and fully supports the initiative taken, which is intended to improve environmental-friendly policies in the area of WEEE.

13. However, the Proposal, as well as the Directive, focuses solely on the environmental risks related to the disposal of WEEE. It does not take into account other additional risks to individuals and/or organisations that may arise from the operations of disposal, reuse or recycling of WEEE, in particular those related to the likelihood of improper acquisition, disclosure or dissemination of personal data stored in the WEEE.

14. It is important to note that Directive 95/46/EC ([8]) applies to 'any operation or set of operations which is performed upon personal data', including their 'erasure or destruction' (Article 2(b)). Disposal of EEE can involve data processing operations. For this reason there is an overlap between the Proposal and the just mentioned Directive, and as such data protection rules could apply to activities covered by the Proposal.

III.2. WEEE's disposal and security measures

15. The EDPS intends to highlight the significant risks that may affect individuals and/or organisations acting as 'data controllers' ([9]) where the WEEE, particularly IT and telecommunications equipments, contain personal data relating to the users of those devices and/or third parties at the time of disposal. The unlawful access to or disclosure of such personal information, sometimes consisting of special categories of data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life (so called 'sensitive data') ([10]), are indeed capable of affecting the privacy and dignity of the persons to whom the information relates, as well as other legitimate interests of those individuals/organisations (e.g. economic ones).

([8]) 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 L 281, 23.11.1995, p. 31).

([9]) For the definition of 'controller' see Article 2(d) of Directive 95/46/EC.

([10]) See Article 8, Directive 95/46/EC.

16. In general terms, the EDPS considers it necessary to emphasise the importance of the adoption of appropriate security measures at every stage (from beginning to end) of the processing of personal data, as repeatedly stated in other opinions ([11]). This applies *a fortiori* in the delicate phase in which the data controller intends to dispose of devices containing personal data.

17. Indeed, the respect of security measures is often a precondition in order to effectively guarantee the right to the protection of personal data.

18. It would therefore be inconsistent to introduce the duty to put in place (sometimes costly) security measures in the ordinary course of processing operations of personal data (as envisaged by Article 17 of Directive 95/46/EC, when applicable ([12])) and then simply omit to consider the introduction of adequate safeguards regarding the disposal of the WEEE.

19. It would be similarly inconsistent to give importance to the issue of data security to the extent that data breach notification had to be introduced via Article 3 of Directive 2009/136/EC ([13]) and then not provide any guarantee or safeguard during the disposal of WEEE as well as in the event of WEEE reuse or recycling.

20. The EDPS regrets that the Proposal does not take into account the potentially damaging effects of the WEEE disposal on the protection of personal data stored in 'used' equipment.

21. This aspect was also not considered in the impact assessment made by the Commission ([14]) although experience has shown that failing to take appropriate security measures in case of WEEE disposal could jeopardise the protection of personal data ([15]). Due to the complexity of the issues involved (for example the multitude of legitimate methods, technologies and stakeholders in the disposal cycle of the WEEE), the EDPS considers that it would have been appropriate to carry out a 'privacy and data protection impact assessment' on the processes related to WEEE disposal.

22. Nevertheless, the EDPS strongly advises that 'Best Available Techniques' for privacy, data protection and security in this area should be developed.

23. As further evidence, during the public consultation prior to the recast of the Directive, issues relating to the security and protection of personal data have sometimes been raised by stakeholders, particularly IT and electronic communications companies ([16]).

24. Finally, it is worth highlighting that some national data protection authorities have published guidelines to minimise the risks which may result from failure to take the necessary security measures, particularly at the disposal of materials subject to the application of the Directive ([17]).

([11]) See Opinion of the EDPS on the Agency for large-scale IT systems (OJ C 70, 19.3.2010, p. 13), points 46 and 47; Opinion on the proposal for a Directive on the application of patient's rights in cross-border healthcare (OJ C 128, 6.6.2009, p. 20), points 27-31.

([12]) See Article 3 of the same Directive.

([13]) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (OJ L 337, 18.12.2009, p. 11).

([14]) Commission Staff Working Paper accompanying the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE) (recast), SEC(2008) 2933, 3.12.2008; but see United Nations University, 2008 Review of Directive 2002/96/EC on waste electrical and electronic equipment (WEEE), European Commission, Belgium, 2007, p. 273 (http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf); 'Data security is also an issue — removing personal data from a hard-drive'.

([15]) See, e.g., BBC's online article 'Children's files on eBay computer', 4 May 2007, reporting that a computer containing personal data about fostering and adopting children was sold on eBay, (http://news.bbc.co.uk/2/hi/uk_news/england/6627265.stm); see also BBC's online article 'Bank customer data sold on eBay' 26 August 2008, reporting that the hard disk containing personal data of one million bank customer was sold on eBay (http://news.bbc.co.uk/2/hi/uk_news/7581540.stm).

([16]) See HP, Stakeholder consultation on the review of Directive 2002/96/EC of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE), pp. 7-8; DELL (draft comments), WEEE Review Policy Options of the stakeholder consultation on the review of Directive 2002/96/EC of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE), p. 2, point 1.1. and 4, point 1.3. (3.6.2008); Royal Philips Electronics Position and Proposal, Stakeholder consultation on the Revision of the WEEE Directive, p. 12 (5.6.2008) (http://circa.europa.eu/Public/irc/env/weee_2008_review/library). See also WEEE Consultation Response, Summary of responses and Government response to fourth consultation on implementation of Directives 2002/96/EC and 2003/108/EC on waste electrical and electronic equipment, December 2006, p. 30: 'Data protection and security. Some waste management companies would like there to be some guidance issued on data protection and security, particularly in light of the fact they will be handling sensitive data' (http://www.berr.gov.uk/files/file35961.pdf).

([17]) Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen, 16. Mai 2007 (http://www.datenschutz-bremen.de/rtf/datenloeschung.rtf); Garante per la protezione dei dati personali, Electrical and Electronic Waste and Data Protection, 13 October 2008 (http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482), also mentioned in the Twelfth Annual Report of the Article 29 Working Party on Data Protection, 16 June 2009, p. 57; see also International Working Group on Data Protection and Telecommunications, Recommendation on Data Protection and E-Waste, Sofia, 12-13.3.2009 (http://www.datenschutz-berlin.de/attachments/650/675.38.14.pdf?1264671551).

25. The EDPS reiterates that Directive 95/46/EC is applicable at the disposal stage of the WEEE containing personal data. Data controllers — in particular those using IT and communications devices — are therefore required to comply with their security obligations to prevent the improper disclosure or dissemination of personal data. To this end and in order not to be held liable for the breach of security measures, the data controller in the public or private sector, with the cooperation of the data protection officers (where present), should adopt appropriate policies for disposal of WEEE containing personal data.

26. Where data controllers disposing of EEE do not have the required skills and/or technical know-how to erase the personal data concerned, they could entrust this task to qualified processors (e.g. assistance centres, equipment manufacturers and distributors) under the conditions provided in Article 17(2), (3) and (4) of Directive 95/46/EC. These processors will in turn certify the performance of the operations in question and/or undertake them.

27. Due to these considerations, the EDPS comes to the conclusion that the recast of the Directive should add data protection principles to the provisions dedicated to the protection of the environment.

28. The EDPS therefore recommends the Council and the European Parliament to include a specific provision in the current Proposal stating that the Directive applies to the disposal of WEEE without prejudice to Directive 95/46/EC.

III.3. **WEEE's reuse or recycle and security measures**

29. Being in a situation allowing autonomous decisions regarding the data held on the EEE, those in charge of disposal operations could be considered as 'data controllers' ([18]). They must therefore adopt internal procedures to avoid unnecessary processing operations on any personal data stored in the WEEE, namely other operations than those strictly necessary to verify the effective elimination of the data contained therein.

30. Moreover, they must not allow unauthorised individuals to gain knowledge of or process data stored on EEE. In particular, when storage media are recycled or reused, and thus re-enter the market, there is an increased risk of improper disclosure or dissemination of personal data, as well as a need to prevent unauthorised access to personal data.

31. The EDPS therefore recommends that the Council and the European Parliament include a specific provision in the current Proposal to prohibit the marketing of used devices which have not previously undergone appropriate security measures, in compliance with state-of-the-art technical standards (for example multi-pass overwriting), in order to erase any personal data they may contain.

III.4. **Privacy and security 'by design'**

32. The forthcoming legal framework on e-waste should not only include a specific provision regarding the wider 'eco-design principle' of the equipment (see Article 4 of the Proposal regarding 'Product design') but also — as previously stated in other EDPS' opinions ([19]) — one regarding the principle of 'Privacy by design' ([20]) or, more precisely in this area, 'security by design' ([21]). As far as possible, privacy and data protection should be integrated into the design of electrical and electronic equipment 'by default', in order to allow users to delete — using a simple means and free of charge — personal data that may be present on devices in the event of their disposal ([22]).

([18]) 'The concept of controller is […] functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a *factual* rather than a formal analysis': see Article 29 Data Protection Working Party, WP 169, Opinion 1/2010 on the concepts of 'controller' and 'processor', adopted on 16 February 2010.

([19]) See, e.g., The EDPS and EU Research and Technological Development. Policy paper, 28 April 2008, p. 2; Opinion of the EDPS on Intelligent Transport Systems (OJ C 47, 25.2.2010, p. 6); Opinion of the EDPS on pharmacovigilance (OJ C 229, 23.9.2009, p. 19).

([20]) In favour of a wide application of the principle see Article 29 Data Protection Working Party — Working Party on Police and Justice, 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, WP 168, adopted on 1 December 2009, p. 3 and 12; see also Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final, p. 8.

([21]) See Communication from the Commission, A European Security Research and Innovation Agenda — Commission's initial position on ESRIF's key findings and recommendations, COM(2009) 691 final, p. 6 and 14.

([22]) See also EDPS, Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy.

33. This approach is clearly supported by Article 3.3(c) of Directive 1999/5/EC ([23]) concerning the design of radio and telecommunications terminal equipment and by Article 14(3) of the Directive 2002/58/EC ([24]).

34. Therefore, producers should 'build in' privacy and security safeguards via technological solutions ([25]). In this framework, initiatives aimed at advising those concerned of the need to erase any personal data before the disposal of WEEE (including producers making free software available for this purpose) should also be fostered and supported ([26]).

IV. **CONCLUSIONS**

35. In consideration of the above, the EDPS recommends that data protection authorities, in particular through the Article 29 Working Party, and the EDPS are closely involved in initiatives related to the disposal of WEEE, through consultation at a sufficiently early stage before the development of relevant measures.

36. Considering the context in which personal data are processed, the EDPS advises that the Proposal should include specific provisions:

— stating that the Directive on WEEE applies without prejudice to Directive 95/46/EC,

— prohibiting the marketing of used devices which have not previously undergone appropriate security measures, in compliance with state-of-the-art technical standards in order to erase any personal data they may contain,

— regarding the principle of 'privacy by design' or 'security by design': as far as possible, privacy and data protection should be integrated into the design of electrical and electronic equipment 'by default', in order to allow users to delete — using simple means and free of charge — personal data that may be present on devices in the event of their disposal.

37. The EDPS strongly recommends, therefore, that the Proposal is amended, in line with Directive 95/46/EC, as follows:

— recital 11: 'In addition, this Directive should apply without prejudice to the legislation on data protection, in particular Directive 95/46/EC. Since electric and electronic equipment (EEE) is a wide product group covering a diverse number of media able to store personal data (such as IT and telecommunications equipment), disposal operations relating to them, in particular reuse and recycling, may present risks of unauthorised access to personal data stored on WEEE. Therefore, as far as possible, privacy and data protection safeguards should be integrated by default into the design of electrical and electronic equipment capable of storing personal data, in order to allow users to delete — simply and without charge — any such data present at the time of disposal.',

— Article 2(3): 'This Directive shall apply without prejudice to the legislation on data protection, in particular Directive 95/46/EC.';

38. In addition, the EDPS considers it appropriate that the following amendments should be taken into consideration:

— Article 4(2): 'Member States shall encourage measures to promote the design and production of electrical and electronic equipment which facilitate the erasure of any personal data contained in the EEE at the time of their disposal',

— Article 8(7): 'Member States shall ensure that any WEEE collected containing personal data which undergoes treatment in order to be recycled or reused is not marketed unless such data has first been removed using the Best Available Techniques.',

([23]) Article 3(3) of 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): '[…] the Commission may decide that apparatus within certain equipment classes or apparatus of particular types shall be so constructed that it incorporates safeguards to ensure that […] the personal data and privacy of the user and of the subscriber are protected'.

([24]) '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'. See also recital 46 of the same Directive, mentioned in footnote 13.

([25]) In favour of this policy perspective see also V. Reding, Keynote Speech at the Data Protection Day, 28 January 2010, European Parliament, Brussels, SPEECH/10/16: 'Businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle. 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. I have seen some encouraging examples, but much more needs to be done'.

([26]) See, e.g., Royal Canadian Mounted Police, B2-002 — IT Media Overwrite and Secure Erase Products (05/2009), in http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/index-eng.htm

— Article 14(6): 'Member States may require that users of EEE containing personal data are given information by producers and/or distributors, e.g. in the instructions for use or at the point of sale, regarding the need to erase personal data which might be contained in the EEE prior to their disposal'.

Done at Brussels, 14 April 2010.

Peter HUSTINX

European Data Protection Supervisor

II

(Information)

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Authorisation for State aid pursuant to Articles 107 and 108 of the TFEU

Cases where the Commission raises no objections

(Text with EEA relevance, except for products falling under Annex I to the Treaty)

(2010/C 280/03)

Date of adoption of the decision	6.7.2010
Reference number of State Aid	N 42/10
Member State	Finland
Region	—
Title (and/or name of the beneficiary)	Tuki maataloustuotannon lopettamiseen
Legal basis	Laki maatalouden harjoittamisesta luopumisen tukemisesta (612/2006), sellaisena kuin se on viimeksi muutettuna lailla (1787/2009); Valtioneuvoston asetus maatalouden harjoittamisesta luopumisen tukemisesta (25/2007)
Type of measure	Early retirement support
Objective	Sectoral development
Form of aid	Direct grant
Budget	EUR 184 million
Intensity	Variable
Duration (period)	1.1.2011-31.12.2014
Economic sectors	Primary production of agricultural products
Name and address of the granting authority	Maa- ja metsätalousministeriö PL 30 FI-00023 Valtioneuvosto Helsinki SUOMI/FINLAND
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

Date of adoption of the decision	20.7.2010
Reference number of State Aid	N 131/10
Member State	Bulgaria
Region	—
Title (and/or name of the beneficiary)	Държавна помощ за компенсиране на загуби, понесени от селскостопанските производители в напълно опустошени райони вследствие на природни бедствия или неблагоприятни климатични условия (нотификация на изменение)
Legal basis	Чл. 12, ал. 1, т. 2 и чл. 12, ал. 2, т. 1, буква „а“ от Закона за подпомагане на земеделските производители, ДВ 58/98 Указания за предоставяне на държавна помощ за компенсиране на загуби в следствие на природни бедствия и неблагоприятни климатични условия
Type of measure	Aid scheme
Objective	Adverse weather conditions, natural disasters or exceptional occurrences
Form of aid	Direct grant
Budget	Overall budget: BGN 600 (in millions)
Intensity	80 %
Duration (period)	Until 31.12.2013
Economic sectors	Agriculture
Name and address of the granting authority	Държавен фонд „Земеделие“ Бул. „Цар Борис III“ № 136 1618 София/Sofia БЪЛГАРИЯ/BULGARIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	9.7.2010
Reference number of State Aid	N 133/10
Member State	Italy
Region	Provincia autonoma di Bolzano
Title (and/or name of the beneficiary)	Disciplina degli aiuti regionali in materia di foreste
Legal basis	Legge Provinciale del 21.10.1996 «Ordinamento Forestale» decreto del Presidente della Giunta provinciale 31 luglio 2000, n. 29 Regolamento all'ordinamento forestale 2000; Programma di sviluppo rurale 2007-2013, misure 111, 122, 123 settore Foreste, 125 Settore Foreste, 226, 227
Type of measure	Aid scheme
Objective	Aid to the forestry sector
Form of aid	Direct grant

Budget	Overall maximum amount: EUR 30 million
Intensity	Max. 100 % of eligible costs
Duration (period)	2010-2013
Economic sectors	Forestry sector
Name and address of the granting authority	Provincia Autonoma di Bolzano Ripartizione Foreste Ufficio economia montana Via Brennero 6 39100 Bolzano BZ ITALIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	4.6.2010
Reference number of State Aid	N 148/10
Member State	Italy
Region	Provincia autonoma di Trento
Title (and/or name of the beneficiary)	Ricostituzione del potenziale forestale e interventi preventivi
Legal basis	Piano di sviluppo rurale della Provincia autonoma di Trento 2007-2013 (Misura 226)
Type of measure	Aid scheme
Objective	Aid to the forestry sector
Form of aid	Direct grant
Budget	Annual maximum expenditure: EUR 3,25 million Overall maximum amount: EUR 13 million
Intensity	Up to 100 % of eligible costs
Duration (period)	31.12.2013
Economic sectors	Forestry sector
Name and address of the granting authority	Provincia autonoma di Trento Piazza Dante 5 38122 Trento TN ITALIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	17.6.2010
Reference number of State Aid	N 209/10
Member State	France
Region	Départements de Charente-Maritime, Vendée et Gironde
Title (and/or name of the beneficiary)	Aides aux exploitants agricoles victimes des inondations marines causées par la tempête Xynthia du 28 février 2010
Legal basis	— Articles L 361-1 et s. du code rural (the budget required for State aid under this scheme will come from the national guarantee fund for agricultural disasters). — Articles 1511-2 à 1511-6 du code général des collectivités territoriales et L 3231-2 et suivants pour les aides des collectivités territoriales. — Arrêté interministériel du 1er mars 2010 de reconnaissance de catastrophe naturelle. — Arrêté interministériel du 11 mars 2010 de reconnaissance de catastrophe naturelle.
Type of measure	Aid scheme
Objective	Aid to provide compensation for losses suffered by farming production
Form of aid	Direct grant
Budget	Max. EUR 43 000 000
Intensity	Maximum 60 %
Duration (period)	4 years
Economic sectors	Agriculture
Name and address of the granting authority	Ministère de l'alimentation, de l'agriculture et de la pêche 78 rue de Varenne 75349 Paris 07 SP FRANCE
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

Authorisation for State aid pursuant to Articles 107 and 108 of the TFEU

Cases where the Commission raises no objections

(Text with EEA relevance, except for products falling under Annex I to the Treaty)

(2010/C 280/04)

Date of adoption of the decision	16.7.2010
Reference number of State Aid	N 414/09
Member State	France
Region	—
Title (and/or name of the beneficiary)	Aides de l'Agence de l'eau Artois-Picardie aux engagements agro-environnementaux dans le bassin Artois Picardie (EAEAP)
Legal basis	Loi nº 2006-1772 du 30 décembre 2006 sur l'eau et les milieux aquatiques (JORF nº 303 du 31 décembre 2006). Proposition de dispositif pour des aides agro-environnementales de l'agence de l'eau Artois-Picardie.
Type of measure	Aid scheme
Objective	Aid to the agro-environmental measures
Form of aid	Direct grant
Budget	Annual expenditure: EUR 21,33 million Overall amount: EUR 64 million
Intensity	Max. 100 % of eligible costs
Duration (period)	2010-2012
Economic sectors	Agricultural sector
Name and address of the granting authority	Agence de l'eau Artois-Picardie 200 rue Marceline BP 818 59508 Douai FRANCE
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	3.2.2010
Reference number of State Aid	N 582/09
Member State	Italy
Region	Sardegna
Title (and/or name of the beneficiary)	Ristrutturazione dell'azienda «Cooperativa viticultori della Planargia»

Legal basis	Legge regionale 19 gennaio 1998, n. 4 «Interventi a favore dì aziende agricole in difficoltà» Legge regionale 29 maggio 2007, n. 2 «Legge finanziaria 2007» — articolo 21 Decreto dell'Assessore n. 2532/DecA/105 del 13.10.2009
Type of measure	Individual aid
Objective	To restructure a firm in difficulty
Form of aid	Direct grant
Budget	EUR 294 540
Intensity	75 %
Duration (period)	After the aid is approved by the Commission
Economic sectors	Agriculture (wine)
Name and address of the granting authority	Assessorato dell'agricoltura e riforma agro-pastorale Via Pessagno 4 09126 Cagliari CA ITALIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	20.7.2010
Reference number of State Aid	NN 26/10
Member State	Czech Republic
Region	—
Title (and/or name of the beneficiary)	Vrácení části spotřební daně na pohonné hmoty spotřebované při zemědělské produkci (změna režimu podpory č. N 678/07)
Legal basis	Zákon č. 353/2003 Sb., o spotřebních daních, ve znění pozdějších předpisů Vyhláška 48/2008 Sb., o způsobu výpočtu nároku na vrácení spotřební daně zaplacené v cenách některých minerálních olejů spotřebovaných v zemědělské prvovýrobě
Type of measure	Scheme
Objective	Aid linked to tax exemptions under Directive 2003/96/EC
Form of aid	Tax advantage
Budget	Total: CZK 6 800 million (approximately EUR 272 million) Annual: CZK 1 700 million (approximately EUR 68 million)
Intensity	60 % of eligible expenses
Duration (period)	Until 31 December 2013

Economic sectors	Agricultural sector
Name and address of the granting authority	Ministerstvo zemědělství Těšnov 17 117 05 Praha 1 ČESKÁ REPUBLIKA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Date of adoption of the decision	16.7.2010
Reference number of State Aid	N 213/10
Member State	Estonia
Region	—
Title (and/or name of the beneficiary)	Eesti maaelu arengukava 2007–2013 meede 2.7 „Natura 2000 toetus erametsamaale”
Legal basis	Eesti maaelu arengukava 2007–2013, peatükk 5.3.2.2; Põllumajandusministri 11.3.2010. aasta määrus nr 26 „Natura 2000 alal asuva erametsamaa kohta antava toetuse saamise nõuded, toetuse taotlemise ja taotluse menetlemise täpsem kord”; Euroopa Liidu ühise põllumajanduspoliitika rakendamise seadus
Type of measure	Aid to forestry sector
Objective	Forestry
Form of aid	Direct grant
Budget	Total budget of EEK 326 million (approximately EUR 20,8 million)
Intensity	Up to 100 % of eligible costs
Duration (period)	From the date of the Commission decision until 31 December 2013
Economic sectors	Forestry
Name and address of the granting authority	Põllumajanduse Registrite ja Informatsiooni Amet Narva 3 51009 Tartu EESTI/ESTONIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

---

Authorisation for State aid pursuant to Articles 107 and 108 of the TFEU

Cases where the Commission raises no objections

(Text with EEA relevance, except for products falling under Annex I to the Treaty)

(2010/C 280/05)

Date of adoption of the decision	12.8.2010
Reference number of State Aid	N 83/10
Member State	Italy
Region	Sardegna
Title (and/or name of the beneficiary)	Aiuto alla ristrutturazione a favore dell'Unione Pastori Società Cooperativa Agricola, registrata nella Z.I Taccu — Nurri Cagliari
Legal basis	Legge regionale 19 gennaio 1998 «Interventi a favore delle aziende agricole in difficoltà» Articolo 21 della legge regionale 29 maggio 2007, n. 2 Decreto regionale n. 343/DecA/7 del 4 febbraio 2010
Type of measure	Individual aid
Objective	Restructuring of a medium-sized enterprise
Form of aid	Direct grant
Budget	EUR 1 million
Intensity	33,3 % of the total restructuring costs (EUR 3 million)
Duration (period)	Ad hoc aid
Economic sectors	Agriculture
Name and address of the granting authority	Regione Autonoma Sardegna Assessorato dell'Agricoltura Via Pessagno 4 09125 Cagliari CA ITALIA
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

Authorisation for State aid pursuant to Articles 107 and 108 of the TFEU

Cases where the Commission raises no objections

(Text with EEA relevance, except for products falling under Annex I to the Treaty)

(2010/C 280/06)

Date of adoption of the decision	7.4.2010
Reference number of State Aid	N 716/09
Member State	Greece
Region	Περιοχές που επλήγησαν από τις πυρκαγιές του 2009
Title (and/or name of the beneficiary)	Πρόγραμμα κρατικών οικονομικών ενισχύσεων για την αντιστάθμιση ζημιών από πυρκαγιές έτους 2009
Legal basis	Σχέδιο ΚΥΑ για τη λήψη μέτρων υπέρ των παραγωγών της χώρας των οποίων οι γεωργοκτηνοτροφικές τους εκμεταλλεύσεις ζημιώθηκαν από πυρκαγιές κατά το έτος 2009
Type of measure	Compensation for damage to means of Agricultural production from an exceptional occurrence
Objective	Exceptional occurrences
Form of aid	Direct grant
Budget	Overall budget EUR 8 000 000
Intensity	The producers, that suffered damages of a minimum threshold of 30 %, will have the right to receive aid. The intensity of the aid will depend on the nature of the damaged object and it will range between 50 %-80 %
Duration (period)	From the approval of the scheme until 31 December 2013
Economic sectors	Agricultural sector
Name and address of the granting authority	α. Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων Αχαρνών 2 101 76 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE β. ΕΛΓΑ Μεσογείων 45 115 10 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE
Other information	—

The authentic text(s) of the decision, from which all confidential information has been removed, can be found at:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_en.htm

IV

(Notices)

NOTICES FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

Euro exchange rates [1]

15 October 2010

(2010/C 280/07)

1 euro =

	Currency	Exchange rate		Currency	Exchange rate
USD	US dollar	1,4089	AUD	Australian dollar	1,4142
JPY	Japanese yen	114,28	CAD	Canadian dollar	1,4165
DKK	Danish krone	7,4564	HKD	Hong Kong dollar	10,9300
GBP	Pound sterling	0,87750	NZD	New Zealand dollar	1,8565
SEK	Swedish krona	9,2230	SGD	Singapore dollar	1,8244
CHF	Swiss franc	1,3423	KRW	South Korean won	1 564,64
ISK	Iceland króna		ZAR	South African rand	9,5833
NOK	Norwegian krone	8,0925	CNY	Chinese yuan renminbi	9,3568
BGN	Bulgarian lev	1,9558	HRK	Croatian kuna	7,3355
CZK	Czech koruna	24,515	IDR	Indonesian rupiah	12 530,82
EEK	Estonian kroon	15,6466	MYR	Malaysian ringgit	4,3443
HUF	Hungarian forint	274,18	PHP	Philippine peso	60,847
LTL	Lithuanian litas	3,4528	RUB	Russian rouble	42,5650
LVL	Latvian lats	0,7097	THB	Thai baht	42,015
PLN	Polish zloty	3,9050	BRL	Brazilian real	2,3369
RON	Romanian leu	4,2765	MXN	Mexican peso	17,4580
TRY	Turkish lira	1,9808	INR	Indian rupee	62,1320

[1] *Source*: reference exchange rate published by the ECB.

COMMISSION DECISION

of 14 October 2010

re-launching of the CARS 21 High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union

(2010/C 280/08)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Whereas:

(1) Article 173 of the Treaty assigned the European Union and the Member States the task of ensuring that the conditions necessary for the competitiveness of the Union's industry exist. Article 191 of the TFEU provides that the Union policy on the environment shall contribute to promoting measures preserving, protecting and improving the quality of the environment and combating climate change.

(2) As part of the Commission's industrial policy, the CARS 21 process ('Competitive Automotive Regulatory System for the 21st century'), which was originally launched in 2005, made recommendations for the short-, medium and long-term public policy in the regulatory framework for the European Union automotive industry that enhances global competitiveness and employment while sustaining further progress in safety and environmental performance at a price affordable to the consumer.

(3) In its Communication 'EUROPE 2020 — a European strategy for smart, sustainable and inclusive growth' [1] the Commission presents proposals to modernise and to decarbonise the transport sector and to promote new technologies including electric cars. The Flagship Initiative 'An industrial policy for the globalisation era' aims to establish an industrial policy creating the best environment to maintain and develop a strong, competitive and diversified industrial base in Europe as well as promoting sustainability by supporting the transition of manufacturing sectors to greater energy and resource efficiency. The Flagship Initiative 'Resource Efficient Europe' will encourage wide-ranging infrastructure measures such as the deployment of grid infrastructures of electrical mobility, intelligent traffic management and above all promoting new technologies including electric and hybrid cars.

(4) The Communication of the Commission 'A European strategy on clean and energy efficient vehicles' [2] defines short- to long-term goals to support research and innovation, to seek solutions of power generation and distribution, to stimulate employment and to encourage market uptake of green vehicles by consumers.

(5) It is therefore necessary to set up a group of experts in the field of competitiveness and sustainable growth of the European Union automotive industry, building on the CARS 21 process, and to define its tasks and structure.

(6) The group should help to identify policies and measures at European Union level, national level and by other stakeholders fostering the competitiveness and sustainable growth of the European Union automotive industry.

(7) The group should be composed of representatives of the European Parliament, the Commission, the Member States and relevant stakeholders of industry and civil society, in particular representatives of consumers, trade unions and non-governmental organisations.

(8) Rules on disclosure of information by members of the group should be provided for, without prejudice to the Commission's rules on security as set out in the Annex to Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure [3].

(9) Personal data should be processed in accordance with 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 [4].

(10) It is appropriate to fix a period for the application of this Decision. The Commission will in due time consider the advisability of an extension,

HAS DECIDED AS FOLLOWS:

Article 1

Group

A High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union, hereinafter referred to as 'the group', previously existing on an informal basis under the title 'Competitive Automotive Regulatory System for the 21st century', is hereby relaunched.

[1] COM(2010) 2020.
[2] COM(2010) 186.
[3] OJ L 317, 3.12.2001, p. 1.
[4] OJ L 8, 12.1.2001, p. 1.

Article 2

Tasks

The group's tasks shall be:

1. to assist the Commission in questions related to the competitiveness and sustainable growth of the automotive industry;

2. to conduct economic and statistical analysis of the factors driving the structural changes in the automotive industry as well as other factors that influence the competitive position of the European Union automotive industry;

3. to assist the Commission in implementing the policy set out by the EUROPE 2020 strategy, its flagship initiative on a resource efficient Europe, its flagship initiative on an industrial policy for the globalisation era and the Communication on clean and energy efficient vehicles COM(2010) 186 as to achieve the goal of maintaining a competitive and sustainable European Union automotive industry;

4. to contribute to ensuring a smooth and balanced economic and social transition, through a pro-active anticipation and management of restructuring processes, skills needs and the related qualification needs, taking into account the results of the 'European Partnership for the Anticipation of Change in the Automotive sector';

5. to formulate a set of sector-specific policy recommendations addressed to policy makers at the European Union and national level, as well as to the industry and civil society organisations;

6. to develop principles of good conduct in order to promote transparency in commercial and contractual relations between the parties to vertical agreements in the motor vehicle sector;

7. to advise on specific aspects of the implementation of the Commission's 2020 Strategy for smart, sustainable and inclusive growth.

Article 3

Membership — Appointment

1. The group shall be composed of up to 40 members.

2. The members shall be individuals appointed in a personal capacity. Each member shall nominate a personal representative to a permanent preparatory sub-group hereafter referred to as 'the preparatory sub-group'.

3. The members shall be appointed by the Commission from high level stakeholders with competence and responsibility in areas which are related to the competitiveness and sustainable growth of the EU automotive industry. The composition shall reflect a balanced representation of different stakeholders. They shall include representatives of the European Parliament, the Commission, the Member States, the actors in the industrial value chain, trade unions and of civil society (non-governmental organisations and consumers).

4. Members are appointed for two years. They shall remain in office until they are replaced or their term of office ends. Their term of office may be renewed.

5. Members who are no longer capable of contributing effectively to the group's deliberations, who resign or who do not comply with the conditions set out in Article 339 of the Treaty may be replaced for the remainder of their term of office.

6. The names of individuals appointed in a personal capacity shall be published in the Register of Commission expert groups and other similar entities, hereinafter referred to as 'Register'.

7. Personal data shall be collected, processed and published in accordance with Regulation (EC) No 45/2001.

Article 4

Operation

1. The group shall be chaired by a representative of the Commission.

2. The preparatory sub-group shall prepare the discussions, position papers and advice for actions and policy measures to be recommended by the group. To that end, it shall work in close contact with the competent Commission services.

3. The group may, in agreement with the services of the Commission, set up working groups, in addition to the preparatory sub-group, to examine specific questions related to the tasks of the group and on the basis of terms of reference defined by the group. Such working groups shall be disbanded as soon as their mandate is fulfilled.

4. The Commission's representative may invite on an ad hoc basis experts or observers from outside the group with specific competence in a subject on the agenda to participate in the work of the group sub-group or working groups. In addition, the Commission's representative may give observer status to individuals, organisations as defined in rule 8(3) of the horizontal rules on expert groups, EU agencies and accession countries.

5. Members of expert groups and their representatives, as well as invited experts and observers, shall comply with the obligations of professional secrecy laid down by the Treaties and their implementing rules, as well as with the Commission's rules on security regarding the protection of EU classified information, laid down in the Annex to Commission Decision 2001/844/EC, ECSC, Euratom. Should they fail to respect these obligations, the Commission may take all appropriate measures.

6. Information obtained by participating in deliberations or work of the group or ad hoc groups or sub-groups shall not be divulged if, in the opinion of the Commission, that information relates to confidential matters.

7. The meetings of the group, preparatory sub-group and working groups shall be held on the Commission premises. The Commission shall provide secretarial services. Other Commission officials with an interest in the proceedings may attend meetings of the group, the preparatory sub-group and working groups.

8. The group shall adopt its rules of procedure on the basis of the standard rules of procedure adopted by the Commission ([1]).

9. The Commission publishes relevant information on the activities carried out by the group either by including it in the Register or via a link from the Register to dedicated website. The final report shall be published as soon as possible after the final meeting of the group.

Article 5

Meeting expenses

1. Participants in the activities of the group shall not be remunerated for the services they render.

2. Travel and subsistence expenses incurred by participants in the activities of the group shall be reimbursed by the Commission in accordance with the provisions in force within the Commission.

3. Those expenses shall be reimbursed within the limits of the available appropriations allocated under the annual procedure for the allocation of resources.

Article 6

Applicability

This Decision shall apply until 14 October 2012.

Done at Brussels, 14 October 2010.

For the Commission
Antonio TAJANI
Vice-President

([1]) OJ L 55/61, 5.3.2010, p. 61.

V

(Announcements)

PROCEDURES RELATING TO THE IMPLEMENTATION OF COMPETITION POLICY

EUROPEAN COMMISSION

Prior notification of a concentration

(Case COMP/M.5927 — BASF/Cognis)

(Text with EEA relevance)

(2010/C 280/09)

1. On 8 October 2010, the Commission received a notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 [1] by which BASF SE ('BASF', Germany) acquires within the meaning of Article 3(1)(b) of the Merger Regulation sole control of Cognis GmbH ('Cognis', Germany), by way of purchase of shares.

2. The business activities of the undertakings concerned are:

— for BASF: chemicals, plastics, performance products, agricultural and functional solutions, oil and gas,

— for Cognis: specialty chemicals and nutritional ingredients.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope the EC Merger Regulation. However, the final decision on this point is reserved.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by e-mail to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.5927 — BASF/Cognis, to the following address:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

---

[1] OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').

Prior notification of a concentration

(Case COMP/M.5982 — CVCII/Advance Properties/Huvepharma)

Candidate case for simplified procedure

(Text with EEA relevance)

(2010/C 280/10)

1. On 8 October 2010, the Commission received a notification of a proposed concentration pursuant to Article 4 and following a referral pursuant to Article 4(5) of Council Regulation (EC) No 139/2004 [1] by which the undertakings Citigroup Venture Capital International Investment G.P. Limited ('CVCII', Jersey), controlled by Citigroup, Inc. (USA), and Advance Properties OOD ('Advance Properties', Bulgaria) acquire within the meaning of Article 3(1)(b) of the Merger Regulation joint control of Huvepharma AD ('Huvepharma', Bulgaria), currently under sole control of Advance Properties, by way of purchase of shares.

2. The business activities of the undertakings concerned are:

— Citigroup: provision of financial services including banking services, brokerage and the management of private equity funds,

— Advance Properties: investments in the fields of pharmaceuticals, real estate, energy and shipping businesses,

— Huvepharma: pharmaceuticals with a focus on animal health and nutrition products.

3. On preliminary examination, the Commission finds that the notified transaction could fall within the scope of the EC Merger Regulation. However, the final decision on this point is reserved. Pursuant to the Commission Notice on a simplified procedure for treatment of certain concentrations under the EC Merger Regulation [2] it should be noted that this case is a candidate for treatment under the procedure set out in the Notice.

4. The Commission invites interested third parties to submit their possible observations on the proposed operation to the Commission.

Observations must reach the Commission not later than 10 days following the date of this publication. Observations can be sent to the Commission by fax (+32 22964301), by email to COMP-MERGER-REGISTRY@ec.europa.eu or by post, under reference number COMP/M.5982 — CVCII/Advance Properties/Huvepharma, to the following address:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

---

[1] OJ L 24, 29.1.2004, p. 1 (the 'EC Merger Regulation').
[2] OJ C 56, 5.3.2005, p. 32 ('Notice on a simplified procedure').

Communication from the Minister for Economic Affairs of the Kingdom of the Netherlands pursuant to Article 3(2) of Directive 94/22/EC of the European Parliament and of the Council on the conditions for granting and using authorisations for the prospection, exploration and production of hydrocarbons

(2010/C 280/11)

The Minister for Economic Affairs hereby gives notice that an application has been received for authorisation to prospect for hydrocarbons in a segment of block P18 as indicated on the map attached as Annex 3 to the Mining Regulation (Mijnbouwregeling) (Government Gazette (Staatscourant) 2002, No 245). The area in question is to be designated block segment P18b.

With reference to the Directive mentioned in the introduction and Article 15 of the Mining Act (Mijnbouwwet) (Bulletin of Acts and Decrees (Staatsblad) 2002, No 542), the Minister for Economic Affairs hereby invites interested parties to submit a competing application for authorisation to prospect for hydrocarbons in block segment P18b of the Dutch continental shelf.

Block segment P18b is delimited by the parallel arcs between vertex pairs A-B and H-I, the meridian arc between vertices B-C, G-H and A-I, by the great circles between vertices C-D and E-F, by arc 1 through points D and E and arc 2 through points F and G.

The coordinates of the vertices are as follows:

vertex	°	′	″ O.L.	°	′	″ N.B.
A	3	40	0,000	52	10	0,000
B	3	47	0,000	52	10	0,000
C	3	47	0,000	52	4	21,072
D	3	47	16,385	52	4	16,801
E	3	51	32,620	52	6	15,485
F	3	51	40,829	52	6	37,449
G	4	0	0,000	52	4	48,172
H	4	0	0,000	52	0	0,000
I	3	40	0,000	52	0	0,000

Arc 1 has a centre with coordinates 3° 54′ 0,000″ O.L., 52° 1′ 30,000″ N.B. and a radius of 5 nautical miles.

Arc 2 has a centre with coordinates 3° 53′ 34,000″ O.L., 52° 1′ 46,000″ N.B. and a radius of 5 nautical miles.

The above vertices are defined by their geographical coordinates, calculated according to the European Terrestrial Reference System.

Block segment P18b covers an area of 313,2 km^2.

The Minister for Economic Affairs is the competent authority for the granting of authorisations. The criteria, conditions and requirements referred to in Articles 5(1), 5(2) and 6(2) of the above-mentioned Directive are set out in the Mining Act (Bulletin of Acts and Decrees 2002, No 542).

Applications may be submitted during the 13 weeks following the publication of this notice in the *Official Journal of the European Union* and should be sent to:

The Minister for Economic Affairs
For the attention of J. C. De Groot, Director for the Energy Market
ALP/562
Bezuidenhoutseweg 30
Postbus 20101
2500 EJ Den Haag
NEDERLAND

Applications received after the expiry of this period will not be considered.

A decision on the applications will be taken not later than 12 months after this period has expired.

Further information can be obtained by calling Mr E. J. Hoppel on the following telephone +31 703797088.

CORRIGENDA

Corrigendum to publication of the application for recognition of a traditional term as provided for in Article 33 of Commission Regulation (EC) No 607/2009

(Official Journal of the European Union C 275 of 12 October 2010)

(2010/C 280/12)

On pages 11, 13 and 15, the phrase 'Competent authority of the Member State:' should be deleted.

Corrigenda

EN

2010 SUBSCRIPTION PRICES (excluding VAT, including normal transport charges)

EU Official Journal, L + C series, paper edition only	22 official EU languages	EUR 1 100 per year
EU Official Journal, L + C series, paper + annual CD-ROM	22 official EU languages	EUR 1 200 per year
EU Official Journal, L series, paper edition only	22 official EU languages	EUR 770 per year
EU Official Journal, L + C series, monthly CD-ROM (cumulative)	22 official EU languages	EUR 400 per year
Supplement to the Official Journal (S series), tendering procedures for public contracts, CD-ROM, two editions per week	multilingual: 23 official EU languages	EUR 300 per year
EU Official Journal, C series — recruitment competitions	Language(s) according to competition(s)	EUR 50 per year

Subscriptions to the *Official Journal of the European Union*, which is published in the official languages of the European Union, are available for 22 language versions. The Official Journal comprises two series, L (Legislation) and C (Information and Notices).

A separate subscription must be taken out for each language version.

In accordance with Council Regulation (EC) No 920/2005, published in Official Journal L 156 of 18 June 2005, the institutions of the European Union are temporarily not bound by the obligation to draft all acts in Irish and publish them in that language. Irish editions of the Official Journal are therefore sold separately.

Subscriptions to the Supplement to the Official Journal (S Series — tendering procedures for public contracts) cover all 23 official language versions on a single multilingual CD-ROM.

On request, subscribers to the *Official Journal of the European Union* can receive the various Annexes to the Official Journal. Subscribers are informed of the publication of Annexes by notices inserted in the *Official Journal of the European Union*.

CD-Rom formats will be replaced by DVD formats during 2010.

Sales and subscriptions

Subscriptions to various priced periodicals, such as the subscription to the *Official Journal of the European Union*, are available from our commercial distributors. The list of commercial distributors is available at:

http://publications.europa.eu/others/agents/index_en.htm

EUR-Lex (http://eur-lex.europa.eu) offers direct access to European Union legislation free of charge. The *Official Journal of the European Union* can be consulted on this website, as can the Treaties, legislation, case-law and preparatory acts.

For further information on the European Union, see: http://europa.eu

Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN