Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on standards of quality and safety of human organs intended for transplantation

(2009/C 192/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to 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,

Having regard to the request for an opinion in accordance with Article 28 (2) of Regulation (EC) No 45/2001 sent to the EDPS on 8 December 2008,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

The proposal for a Directive on standards of quality and safety of human organs intended for transplantation

1. On 8 December 2008, the Commission adopted a Proposal for a Directive of the European Parliament and of the Council on standards of quality and safety of human organs intended for transplantation (hereinafter: the proposal) ([1]). The proposal was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001.

2. The proposal aims at ensuring high standards of quality and safety for human organs intended for transplantation, in order to ensure a high level of human health protection. In particular, the proposal:

   — Sets out basic quality and safety requirements needed in the Member States' transplant systems, and provides for the creation or designation of a competent national authority for ensuring compliance with these requirements. To this end, national quality programmes will be established for the procurement and transfer of human organs in all countries, including inter alia a system for the *reporting of serious adverse events and reactions*, as well as a *traceability mechanism* to ensure that all organs can be traced from donation to reception and vice versa.

   — Provides for the protection of donors and recipients. Especially with regard to living donors, the proposal includes measures for the evaluation of the health of donor and comprehensive information about the risks to donation, the introduction of *registers of living donors*, as well as measures to ensure the altruistic and voluntary donation of organs by living donors.

   — Facilitates cooperation between Member States and *cross-border exchanges of organs* (also between Member States and third countries), standardising the collection of relevant information for the organ's characteristics and establishing a mechanism for the transmission of information.

3. The implementation of the proposed organ donation and transplantation scheme requires the processing of personal data relating to health (health data) of the organs' donors and receivers by the authorised organisations and healthcare professionals of the different Member States. These data are deemed as sensitive and fall under the stricter rules of data protection as laid down in Article 8 of Directive 95/46/EC on special categories of data.

4. More specifically, the donors' data are being processed in the procurement organisations that perform the donor and organ characterisation and, thus, define whether the organ under consideration is appropriate for transplantation (a list of these data is provided in the Annex to the proposal). The recipients' (patients) data are being processed in the transplantation centres where the operation actually takes place. Although there is no communication of the donor's data to the recipient (and vice versa), there is a requirement for the national competent authorities to maintain full traceability of the organ from the donor to recipient (and vice versa), which should be possible also in the cases of cross-border exchange of organs.

EDPS consultation

5. The EDPS welcomes the fact that he is consulted and that reference to this consultation is made in the preamble of the proposal, in accordance with Article 28 of Regulation (EC) No 45/2001.

([1]) COM(2008) 818 final.

6. The proposal will advance organ donation and transplantation procedures, with a final aim of increasing organ availability and decreasing mortality in organs waiting lists. It is complementing the existing legislative framework with regard to the use of biological materials of human origin ([1]). Moreover, it can be seen as part of the overall EC approach towards setting different types of common standards for the provision of healthcare services at the Member States, with a basic aim of promoting cross-border availability of these services across Europe ([2]). As already stated in his Opinion on patients' rights in cross-border healthcare, the EDPS supports such an approach. However, he emphasises again the need for a well coordinated and uniform data protection perspective throughout the various healthcare related initiatives ([3]).

7. The proposal has already considered the data protection needs arising both for the donors, and the recipients of organs. The most important element is the requirement to keep the donors' and recipients' identity confidential (recitals 11 and 15, Articles 10 and 17). A number of general references to data protection can furthermore be found in some parts of the proposal (recital 17, Articles 16, 4(3)(a), 15(3) and 19(1)(a), Annex), as well as more specific references on the need to cooperate with the national Data Protection Authorities (Articles 18(f) and 20(2)).

8. The EDPS welcomes the aforementioned content. He would however like to express his concerns about some of the provisions which are not clearly defined or elaborated, and are therefore leading to ambiguities, which could potentially affect the uniform implementation of the proposal by the Member States.

9. More specifically, the sometimes conflicting use of the concepts of 'organs traceability' and 'anonymity of donors and recipients' is an issue which requires further clarification and precision. In connection with this, the need to adopt enhanced security measures for the protection of the donors' and recipients' data at Member States level should be further stressed, to guarantee a reinforced data protection level in the different European countries, as well as to ensure data protection in the cross-border exchange of organs (within or outside Europe).

10. The present Opinion will elaborate further on the above mentioned issues, with the aim of improving the current data protection related content of the proposal, both in terms of clarity and consistency.

II. CLARIFYING THE CONCEPTS OF TRACEABILITY AND ANONYMITY

The applicability of Directive 95/46/EC

11. According to Article 2(a) of Directive 95/46/EC on the protection of personal data, 'personal data' means: 'any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

12. Biological materials of human origin, like organs, tissues, cells or blood, can be defined as material that can be extracted from the human body. It is questionable whether these materials as such can be considered as personal data. However, it is undisputed that such materials can be used as *sources* of personal information about their holder. The extraction of such information is often the purpose of the processing of biological materials. And even without such a purpose, the biological materials are often accompanied by such extracted information. In those situations the rules of Directive 95/46/EC apply ([4]). That is to say, as long as the holder of the biological material is an *identified* or *identifiable* (natural) person.

13. Recital 26 of Directive 95/46/EC explains how to determine whether a person is identifiable: 'account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person'. The same Recital furthermore explains that the rules of Directive 95/46/EC do not apply if the information relates to a person who is not or no longer identifiable: such data are considered as *anonymous*.

14. In Recommendation (2006)4, the Council of Europe has addressed the specific issue of identifiability of biological materials, making a distinction between identifiable and non-identifiable biological materials ([5]).

15. According to the recommendation *identifiable biological materials* are 'those biological materials which, alone or in combination with associated data, allow the identification of the persons concerned either directly or through the use of a code' ([6]). In the latter case, the user of the biological

([1]) This framework includes Directives 2002/98/EC, 2004/33/EC, 2005/61/EC and 2005/62/EC for blood and blood products, and Directives 2004/23/EC, 2006/17/EC and 2006/86/EC for human tissues and cells.

([2]) See also the Proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, COM(2008) 414 final.

([3]) EDPS Opinion of 2 December 2008 on the proposal for a Directive on the application of patient's rights in cross-border healthcare.

([4]) Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, p. 9.

([5]) Recommendation Rec(2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin.

([6]) Article 2(i) of Recommendation Rec(2006) 4.

materials may either have access to the code (coded materials) or not have access to the code, which is under the control of a third party (linked anonymised materials). In its opinion 4/2007 on the concept of personal data, the Article 29 Working Party (hereinafter: WP29) used the notion of *retraceable pseudonymised data* to describe indirectly identifiable information on individuals, which can still be used to backtrack to and identify the individuals under predefined conditions ([1]). *Key-coded data* are mentioned as an example, where personal data are earmarked by a code, while the key making the correspondence between the code and the common identifiers of the individuals is kept separately. If the codes used are unique for each specific person, identification is possible through the key applied for the coding.

16. The recommendation also refers to the *non-identifiable biological materials* (or unlinked anonymised materials) as 'those biological materials which, alone or in combination with associated data, do not allow, with reasonable efforts, the identification of the persons concerned' ([2]). These would indeed be considered anonymous data, as defined by Directive 95/46/EC.

17. It follows from the foregoing that Directive 95/46/EC applies to the collection, storage and processing of identifiable organs and the subsequent extraction of information from such organs, for as long as it remains possible, with due account of all means likely reasonably to be used, to identify the person concerned. As will be shown, the permanent traceability of organs as envisaged in the proposed directive will keep the persons identifiable throughout the whole process.

Traceability versus anonymity of human organs

18. Traceability of a biological material is the possibility to backtrack to the holder of the material and, thus, identify him/her. To put it in other words, whenever traceability of the holders of the biological materials is possible, either in a direct or indirect way, these can be considered as identifiable and vice versa. The concepts of 'traceability' and 'identifiably' are therefore in principle strongly connected to each other. On the contrary, traceability and anonymity of data cannot appear at the same time. They are opposite to each other. If certain information is truly anonymous it is not possible to identify and trace back the individuals.

19. In the context of the current proposal, traceability is a mandatory requirement to be established in the framework of the Member States national quality programmes in a twofold way, i.e. both to the donors and to the recipients. This means that, although information about donors and recipients is kept confidential, the organs related information is identifiable. This is also included in the proposal's definition on traceability in Article 3: 'the ability for a competent authority to locate and identify the organ at each stage in the chain from donation to transplantation or disposal, which under specified circumstances in this Directive is authorised to identify the donor and the procurement organisation, identify the recipients at the transplantation centre, locate and identify all relevant non-personal information relating to products and materials coming into contact with that organ'.

20. Moreover, Article 10 of the proposal on traceability states in its first paragraph that 'Member States shall ensure that all organs procured and allocated in their territory can be traced from the donor to recipient and vice versa in order to safeguard the health of donors and recipients'. Paragraph 3 of the same article states that 'Member States shall ensure that: (a the competent authorities or other bodies involved in the chain from donation to transplantation or disposal keep the data needed to ensure traceability at all stages of the chain from donation to transplantation or disposal in accordance with the national quality programmes, (b data required for full traceability is kept for a minimum of 30 years after donation. Such data storage may be stored in electronic form'.

21. Although the traceability process is subject to implementing measures (see Article 25 of the proposal), an indirect identification scheme of the donors and recipients seems the most likely solution, following or at least being interoperable with Directive 2004/23/EC ([3]) on tissues and cells and the European identifying code established therein ([4]). In such a case, the processing relating to

([1]) Article 29 Data Protection Working Party, Opinion 4/2007, p. 18.
([2]) Article 2(ii) of Recommendation Rec(2006) 4.

([3]) Since organ donors are very often tissue donors, there is a need to trace and report any unexpected adverse reaction also in the tissue vigilance system, and, thus, interoperability with the indirect identification method used in this system is required. See: Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells, OJ L 102/48, 7.4.2004, and Commission Directive 2006/86/EC of 24 October 2006 implementing Directive 2004/23/EC of the European Parliament and of the Council as regards traceability requirements, notification of serious adverse reactions and events and certain technical requirements for coding, processing, preservation, storage and distribution of human tissues and cells, OJ L 294/32, 25.10.2006.

([4]) This code includes a unique identification number for each donation, which, together with the tissue establishment and product identification, can trace back to the donors and recipients. More specifically, according to Article 10 of Directive 2006/86/EC, 'a single European identifying code shall be allocated to all donated material at the tissue establishment, to ensure proper identification of the donor and the traceability of all donated material and to provide information on the main characteristics and properties of tissues and cells'. As described in the Annex VII to this Directive, the code has two parts: (a donation identification, including a unique ID number for the donation and the identification of the tissue establishment, and (b product identification, including product code, split number and expiry date.

donors and recipients in the context of the proposal concerns linked anonymised biological materials or in data protection terminology retraceable pseudonymised data (see above in point 15) to which the provisions of Directive 95/46/EC apply.

22. It is noted however that, despite the clear traceability and identifiability requirements, the proposal in some of its parts uses the term 'anonymity' or 'anonymous data' to refer to the donors' and recipients' data. As follows from the previous points, this is contradictory and highly confusing. ([1])

23. More specifically, paragraph 2 of Article 10 of the proposal, which sets the need for a donor identification system, states that 'Member States shall ensure the implementation of a donor identification system that can identify each donation and each of the organs associated with it. Member States shall ensure that this donor identification system is designed with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for pseudonymisation or rendering individuals anonymous' ([2]). The EDPS is of the opinion that the underlined terms in this particular paragraph are in conflict with the concept of traceability, since there is no possibility to have traceable and identifiable data when donors and recipients are rendered anonymous. Besides, it is remarkable that this paragraph refers to donor identification, whereas the recipient identification (which is also part of the process) is not mentioned at all.

24. The aforementioned contradiction is even more apparent in Article 17 on Anonymisation of donors and recipients, which states that: 'Member States shall take all necessary measures to ensure that all personal data of donors and recipients processed within the scope of this Directive are rendered anonymous so that neither donors nor recipients remain identifiable'. This Article is entirely in conflict with the proposal's articles on traceability.

Confidentiality instead of anonymity

25. The EDPS understands that the term anonymity is actually used to stress the need for enhanced *confidentiality* ([3]) of the donors' and recipients' data, meaning that information is accessible only to those authorised to have access. The EDPS assumes that anonymisation is more specifically used as implying an indirect identification scheme used for the donors and recipients ([4]), which can also be distracted from the way in which this term is used in Directive 2004/23/EC on tissues and cells. As stated earlier, however, anonymity is not the correct term to be used.

26. An example of how both data protection and traceability can be addressed in a transplantation process can be found in the Council of Europe Additional Protocol to the Convention on human rights and biomedicine ([5]). There, the concept of confidentiality is used instead of anonymity. More specifically Article 23(1) of the protocol states that 'all personal data relating to the person from whom organs or tissues have been removed and those relating to the recipient shall be considered to be confidential. Such data may only be collected, processed and communicated according to the rules relating to professional confidentiality and personal data protection'. Paragraph 2 of the same article continues as follows: 'the provisions of paragraph 1 shall be interpreted without prejudice to the provisions making possible, subject to appropriate safeguards, the collection, processing and communication of the necessary information about the person from whom organs or tissues have been removed or the recipient(s) of organs and tissues in so far as this is required for medical purposes, including traceability, as provided for in Article 3 of this protocol'.

27. Based on the foregoing, the EDPS recommends to alter the language in certain parts of the proposal in order to avoid ambiguity and to explicitly reflect the fact that the data are not anonymous but should be processed under strong confidentiality and security rules. More specifically, the EDPS recommends the following changes:

([1]) This observation was also made by the EDPS in his comments of 19.9.2006 on the public consultation on the future EU action in the area of organ donation and transplantation.

([2]) Own emphasis.

([3]) Ensuring that information is accessible only to those authorised to have access (ISO definition, source: http://www.wikipedia.org).

([4]) The term 'anonymisation', depending on the context where it is applied, is sometimes used to imply indirectly identifiable data, like in the case of statistics. This, however, is not correct from a data protection point of view as was explained by the EDPS in his Opinions on the proposal for a Regulation of the European Parliament and of the Council on Community statistics on public health and health safety at work (COM(2007) 46 final), and on the proposal for a Regulation of the European Parliament and of the Council on European Statistics (COM(2007) 625 final).

([5]) Council of Europe, Additional Protocol to the Convention on Human Rights and Biomedicine concerning transplantation of Organs and Tissues of Human Origin, Strasbourg, 24.1.2002, see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG for ratification chart. See also: Council of Europe, Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, Oviedo, 4.4.1997, see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG for ratification chart.

— In recital 15, last sentence: 'In line with the charter and to take account of, as appropriate, the Convention of Human Rights and Biomedicine, organ transplantation programmes should be founded on the principles of voluntary and unpaid donation, altruism of the donor and solidarity between donor and recipient, while ensuring that strict confidentiality rules and security measures are in place for the protection of the donors' and the recipients' personal data'.

— In Article 10, paragraph 2, second and third sentences: 'Member States shall ensure the implementation of a donor and recipient identification system that can identify each donation and each of the organs associated with it. Member States shall ensure that the donor and recipient identification systems are designed and selected in accordance with the aim of collecting, processing or using as little personal data as possible, making in particular use of pseudonymisation methods, as well as that the necessary technical and organisational measures are in place for the security of these data'.

— Article 17 as such could be deleted, incorporating its content (in terms of confidentiality needs) in a new paragraph of Article 16 on the Protection of personal data, confidentiality and security of processing (see point 36 below).

28. Moreover, as will be discussed in the following parts of this Opinion, the EDPS suggests to further outline the need for *reinforced protection* of the donors' and recipients' data through the application of *strong security measures*, both at national and at cross-border level.

III. **STRESSING NATIONAL DATA SECURITY MEASURES**

Basic security needs and requirements

29. As follows from the proposal, the processing of personal data of the donors and recipients mainly takes place at national level, i.e. in the Member States procurement and transplantation centres. It is at this level that the register of living donors is also kept. Although the traceability mechanism has not yet been defined, it can be expected that any codification activity will also occur at national level even in the case that a European coding system is used, since identification of the donors and recipients is only possible through the national competent authorities.

30. It is therefore of utmost importance to implement an information security policy based on *strict and sound security measures* at the relevant national services, especially in order to meet the confidentiality requirements for the donors and recipients set out in the proposal, as well as to safeguard *integrity* ([1]), *accountability* ([2]) and *availability* ([3]) of these data. In this regard, the information security policy should cover elements of physical and logical security focusing, among other, on the control of data entry, access, recording, transfer and communication, as well as data media and storage control.

31. With regard to confidentiality, the medical data of the recipients' ([4]), as well as the data used for the donors' characterisation and follow-up (also in relation to 'expanded donors' ([5])), may reveal sensitive personal information about them, which can affect their social, professional and/or personal life as well. The protection of the donors' identification data is of further importance, where living donors or persons who have provided their consent to donate one or more of their organs after their death could become victims of trafficking of human organs and tissues in case this information is revealed. Integrity of the organs' related data is also crucial, since even a single mistake in the transferred information could be life-threatening for the recipient. The same applies for the accuracy of the donors' health data prior to the transplantation, since these data are used to identify whether the organ is suitable or not. As regards accountability, since so many different organisations are involved in the overall donation and transplantation scheme, there should be a way that all involved entities are aware and can take responsibility of their actions, e.g. in case where donors' identification data is revealed to non-authorised persons or the organs' medical data are not accurate. Last, since the whole system is based on the transfer of the organs related data and the traceability mechanism from donor to recipient, these data should be at the disposal of the

([1]) Ensuring that data is 'whole' or complete, the condition in which data are identically maintained during any operation (such as transfer, storage or retrieval), the preservation of data for their intended use, or, relative to specified operations, the a priori expectation of data quality. Put simply, data integrity is the assurance that data is consistent and correct (source: http://www.wikipedia.org); ensuring that information can only be accessed or modified by those authorised to do so (source: http://searchdatacenter.techtarget.com).

([2]) Liability to account for one's actions; non-repudiation: ensuring that the data has been sent and received by the parties claiming to have sent and received it: the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement (source: http://www.wikipedia.org).

([3]) The degree to which the data can be instantly accessed (source: http://www.pcmag.com).

([4]) It has to be noted that the mere fact that an organ is transplanted to a recipient constitutes sensitive personal data about the health of this person.

([5]) Potential donors, who are not the ideal donor candidates, but could be considered under certain circumstances, e.g. for elderly recipients. See: Commission Staff Working Document accompanying the proposal for a directive of the European Parliament and of the Council on standards of quality and safety of human organs indented for transplantation and the Communication from the Commission Action Plan on Organ Donation and Transplantation (2009-2015): Strengthened cooperation between Member States, Impact Assessment, 8.12.2008.

authorised persons when needed without delay (otherwise non-availability would compromise the sound system's performance).

32. In this respect, appropriate *authorisation mechanisms* should be in place, following specific *access controls policies*, both for the national databases and in the case of cross-border exchanges of organs. These policies should at first be defined at the organisational level, especially with regard to the identification procedures for the donors and recipients (e.g. who has access to what information and under which circumstances). In this way *access rights* will be set out, together with *access scenarios* where these rights can be executed (e.g. circumstances and procedure for disclosing data by the procurement organisation to the competent authority, certain — if any — cases where the identity of the donor needs to be disclosed to the recipient and the procedures for doing it, etc.). In order for the policies to be effective, the persons involved in the processing should be bound with specific *confidentiality rules*.

33. Once these policies are determined, they can be implemented at technical level, i.e. in terms of controlling user access to systems and applications according to the predefined access rights. Proven technologies, like *encryption* and *digital certificates* [1] (e.g. based on *public key infrastructure schemes* [2]), can be used for this. *Role-based authentication mechanisms* can also be applied to restrict the user access rights based on their role (e.g. only doctors should be in the position of modifying the recipients' and donors' medical data into the national databases).

34. Access control should be complemented with possibilities for *logging* users actions (e.g. read and write access to medical data), especially when electronic systems are used. Physical and logical security measures should also be in place to make sure that the donors' and organs' databases are *fully operational* as a central element of the proposed donation and transplantation system. Availability of the data should be considered as a cornerstone of the system. In this regard, the information security policy should be based on a *sound risk analysis and assessment*, and should also include elements as incidents and business continuity management. All these elements should be maintained and improved through regular processes of monitoring and reviewing. *Independent audits* can also increase the effectiveness and improvement of the system, paying especial attention to pseudonymisation, traceability and data transfer practices.

35. The EDPS would like to see more emphasis put on the need for such measures in the context of the proposed Directive.

Enhancement of the proposal's security provisions

36. Article 16 of the proposal on the Protection of personal data, confidentiality and security of processing states that 'Member States shall ensure that the fundamental right to protection of personal data is fully and effectively protected in all organ transplantation activities, in conformity with Community provisions on the protection of personal data, such as Directive 95/46/EC, and in particular Articles 8(3), 16, 17 and 28(2) of that Directive'. The EDPS recommends that a *second paragraph* is added in this article, describing the basic principles for ensuring security at the Member State level, including as a minimum a reference to the following points:

— An information security policy should be in place implementing technical and organisational measures to ensure confidentiality, integrity, accountability and availability of the donors' and recipients' personal data.

— A specific confidentiality and access control policy should be defined for use in all Member States, specifying access rights, roles and responsibilities for all involved parties (donor, procurement organisation, transplantation centre, recipient, national competent authority, cross-border competent authority) throughout the whole traceability chain. Specific data confidentiality guarantees should be in place for the persons involved in the processing, especially if these persons are not bound with the obligation of medical secrecy (e.g. confidentiality codes of conduct and measures focused on awareness).

— The need to address security mechanisms (like encryption and digital certificates) in the national databases should be outlined. Especially with regard to the donors' registers the principle of 'privacy by design' should be applied, in order to include all the necessary security requirements at the initial implementation stages of such developments.

— Procedures should also be established to safeguard the data protection rights of the donors and recipients, especially the rights of access and rectification, as well as the right to information. Special care should also be given to the cases of donors who wish to withdraw their consent or are not accepted (after the donor and organ characterisation) as donors. In this case, a specific procedure and time limit should be defined for the retention of their data.

[1] The electronic equivalent of an ID card that authenticates the originator of a digital signature (source: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

[2] A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates (source: http://www.wikipedia.org).

— The information security policy should also provide measures aimed at guaranteeing the integrity and uninterrupted availability of the data. The role of information security risk assessment should be complemented with the assumption of elements regarding incidents and business continuity management.

— The information security policies should be subjected to regular monitoring and reviewing, including independent audits.

37. The EDPS recommends that the above mentioned elements are included in Article 16 and then further specified as part of the implementing measures of Article 25, especially paragraph 1(a), (b) and (c).

IV. **SAFEGUARDS REGARDING CROSS-BORDER EXCHANGES OF ORGANS**

Security harmonisation across Member States

38. The cross-border exchange of organs will in practice always involve processing of personal data, since, even if coded, the organs remain (indirectly) identifiable through the national competent authorities.

39. The EDPS has already expressed his opinion about the security needs for the protection of personal data in cross-border healthcare within Europe, stressing inter alia the need for harmonising information security policies among Member States in order to achieve a sound data protection level [1]. He recommends that this element is also mentioned in the current proposal and more specifically in Recital (17) where the provision of Directive 95/46/EC on security of processing is mentioned.

Establishment of the traceability system

40. In this specific case, a significant parameter for cross-border data security is the traceability mechanism to be established. To this end, besides the security measures applied at Member State level, special attention should be paid to pseudonymisation possibilities to be used for the identification of donors and recipients (e.g. type of codification, possibility of double codification, etc) and to maintaining interoperability with the tissue and cells identification system.

41. The EDPS recommends that a specific reference on this item is made in Article 25 of the proposed Directive on the implementing measures, amending paragraph 1(b) as follows: 'procedures for ensuring the full traceability of organs, including labelling requirements, while safeguarding confidentiality of donors and recipients throughout the whole traceability process and maintaining interoperability with the tissue and cells identification system.'

Exchange of organs with third countries

42. Security needs are even more important when data are exchanged with third countries where an adequate data protection level cannot always be guaranteed. A specific regime for transfer of personal data to third countries is laid down in Articles 25 and 26 of Directive 95/46/EC. The EDPS is aware of the fact that data protection requirements should not obstruct the fast and efficient transfer of organs, which is a necessity in the system of organ donation and can often even be a matter of life or death. The possibilities of allowing transfers despite the lack of an adequate level of data protection in general in the third country should therefore be explored. One should thereby take into account that due to the indirect nature of the individuals' identification at cross-border level together with the fact that the national competent authorities have the overall supervision of the system, the risks at stake are most probably lower than those arising at national level [2].

43. To this end, the EDPS is of the opinion that the competent authority, who is responsible for the authorisation of such transfers, consults with the national Data Protection Authority in order to develop, in light of the possible derogations indicated in Article 26 of Directive 95/46/EC, the necessary framework for secure, but also fast and efficient transfer of organs' data to and from third countries. The EDPS recommends that a reference on this item is made in Article 21 on the Exchange of organs with third countries or in the relevant recital 15.

Implementing measures

44. As a final remark, the EDPS urges the legislator to ensure that, with regard to Article 25, in all cases where implementing measures affecting data protection and security are considered, all relevant stakeholders are consulted, including the EDPS and the Article 29 Working Party.

V. **CONCLUSIONS**

45. The EDPS has noted the initiative to ensure high standards of quality and safety for human organs intended for transplantation, which can be seen as part of the overall EC approach towards setting common standards to promote cross-border availability of healthcare services across Europe.

46. The proposal has already considered the data protection needs arising for the donors and the recipients of organs, especially with regard to the requirement for keeping their identities confidential. The EDPS regrets however that some of these provisions are vague, ambiguous or general and, for this reason, he recommends a number of amendments to enhance the proposal's data protection related content.

[1] EDPS Opinion of 2 December 2008 on the proposal for a directive on the application of patient's rights in cross-border healthcare.

[2] See Article 29 Data Protection Working Party, Opinion 4/2007, p. 18 on pseudonymised and key-coded data.

47. As a first point, the EDPS notes the existing contradiction between the concepts of traceability and anonymity used within the proposal. In this respect, he recommends specific changes of the language in certain parts of the proposal (namely in recital 15, Article 10 paragraph 2 and Article 17) in order to avoid ambiguity and to explicitly reflect the fact that the data are not anonymous but should be processed under strong confidentiality and security rules.

48. Moreover, he recommends laying more emphasis on the need to adopt strong security measures at national level. This could be done by adding a second paragraph in Article 16 describing the basic principles for ensuring security at the Member State level, and further specifying these principles as part of the implementing measures of Article 25(1). The proposed security principles include:

(a) adoption of an information security policy to ensure confidentiality, integrity, accountability and availability of the donors' and recipients' personal data;

(b) definition of a specific confidentiality and access control policy, together with data confidentiality guarantees for the persons involved in the processing;

(c) addressing security mechanisms in the national databases, based on the principle of 'privacy by design';

(d) establishing procedures to safeguard the data protection rights of the donors and recipients, especially the rights of access and rectification and the right to information, paying special attention to the cases of donors who wish to withdraw their consent or are not accepted as donors;

(e) provision of measures to guarantee integrity and uninterrupted availability of the data;

(f) ensuring regular monitoring and independent audits of the security policies in place.

49. With regard to the cross-border exchange of organs, the EDPS recommends that the need for harmonising information security policies among Member States is mentioned in Recital (17) of the proposal. In addition, special attention should be paid to the pseudonymisation possibilities to be used for the identification of donors and recipients, and to maintaining interoperability with the tissue and cells identification system. The EDPS recommends that a specific reference on this item is made in Article 25(1)(b) of the proposal.

50. Concerning the exchange of organs with third countries, the EDPS recommends to mention in Article 21 or relevant Recital 15 of the proposal that the competent authority will consult with the national Data Protection Authority in order to develop the necessary framework for secure, but also fast and efficient transfer of organs' data to and from the third countries.

51. Finally, the EDPS recommends that in all cases where implementing measures affecting data protection and security are considered, all relevant stakeholders are consulted, including the EDPS and the Article 29 Working Party.

Done in Brussels, 5 March 2009.

Peter HUSTINX

European Data Protection Supervisor