Opinion of the European Data Protection Supervisor

on the Communication from the Commission on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century'

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

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 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[2], and in particular Article 28(2) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 6 December 2012, the Commission adopted a Communication on the 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century' (the Communication)[3]. This Proposal was sent to the EDPS for consultation on 7 December 2012.

2. Before the adoption of the Communication, the EDPS was given the possibility to provide informal comments to the Commission. He welcomes that some of his comments have been taken into account in the Communication.

1.2. Objectives and scope of the Communication and aim of the EDPS Opinion

3. The Communication establishes an eHealth Action Plan for 2012-2020. The Action Plan presents the view that Information and Communication Technologies (ICT) applied to healthcare and well-being can improve the

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM (2012) 736 final.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

efficiency and effectiveness of healthcare systems, empower the individual citizen and unlock innovation in the health and well-being markets.

4. This EDPS Opinion is to be seen in the light of the growing importance of eHealth in the evolving information society and of the ongoing policy debate within the EU on eHealth. The Opinion focuses especially on the implications of the fundamental right to data protection for eHealth initiatives. It also comments on the areas for further action identified in the Communication.

2. ANALYSIS OF THE PROPOSAL

2.1. General comments

2.1.1. Data protection in the Communication and reference to applicable legislation

5. The EDPS welcomes the recognition of the relevance of data protection for eHealth in a subsection to section 4.3 of the Communication, which is named 'Empowering citizens and patients: review of data protection rules' (data protection subsection).

6. The EDPS welcomes the fact that the draft Communication makes reference to the proposed general Data Protection Regulation. However, until the proposed new legislation enters into force -this may take a few years- the current legal framework for data protection will remain applicable.

7. The EDPS therefore recommends the Communication to refer to the current data protection legal framework set forth under Directive 95/46/EC and Directive 2002/58/EC, which contains the relevant data protection principles that are currently applicable. These rules are to be respected for any action to be taken in the short to medium term until the proposed revised Data Protection legislative package will enter into force.

2.1.2. Patients´ empowerment and right to self determination

8. The EDPS welcomes the emphasis put in the Communication on the empowerment of the patient and the respect of his/her right to self-determination. He also welcomes references to the rights to be forgotten and to data portability as foreseen in the proposed Data Protection Regulation. The EDPS wishes to underline that the rights to have access to one's own personal data and to be informed in a clear and transparent manner of how these data are processed through health and well-being technologies also contribute to such empowerment. However, the EDPS notes that the importance of these rights in the context of eHealth has not been made clearer in the Communication. In particular, he therefore encourages the Commission to draw the attention of (data) controllers acting in the field of eHealth to the necessity to provide individuals with clear information about the processing of their data in eHealth applications as the cornerstone of patient empowerment in this area.

2.2. Personal data concerning health

9. Data processing in the context of eHealth and well-being ICT often involves the processing of personal data -of the patients, of any other data subject involved, and of health professionals- in the sense of Article 2(a) of Directive 95/46/EC.

10. The Communication distinguishes between health data and well-being data. The EDPS would like to underline that both categories of data may involve the processing of personal data relating to health.

11. Processing of such data is subject to strict data protection rules as laid down in Article 8 of Directive 95/46/EC and its implementing national laws (and as foreseen in Article 9 of the proposed Data Protection Regulation). The EDPS wishes to underline that this sets a high standard with which compliance must be ensured and wishes to underline the guidance already given to controllers and processors in the area[4].

12. Furthermore, the importance of protecting personal data concerning Health has repeatedly been emphasised by the European Court of Human Rights in the context of Article 8 of the European Convention of Human Rights. The Court has stated: '*The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention*'[5].

2.3. Comments on data protection issues in section 4.3 of the Communication

2.3.1. The role of data protection in eHealth

13. As a first point, the EDPS would like to emphasise that compliance with data protection requirements, in particular in the field of eHealth, should not be seen as a barrier to the deployment of ICT but as a main enabler of trust. These data protection requirements ensure for instance that data are kept accurate, that users are provided with relevant information about the processing operations to be carried out and have the means to exercise a degree of control over their own data, and that appropriate security and confidentiality measures are implemented across the entire chain of processing.

14. Therefore, the EDPS welcomes the second paragraph on page 9 of the Communication stating that *'Effective data protection is vital for building trust in eHealth. It is also a key driver for its successful cross-border deployment, in which harmonisation of rules concerning cross border exchange of health data is essential'* and the reference in footnote 34 to the EDPS Opinion on the Data protection Reform.

[4] See below under Section 2.3.1.

[5] See ECHR 17 July 2008, I v Finland (appl. No 20511/03), paragraph 38 and ECHR 25 November 2008, Armonas v Lithuania (appl. No 36919/02), paragraph 40.

15. The EDPS agrees that it is essential that there must be clear rules on handling health data and believes that the main problem thus far has not been the lack of clarity of these rules at national level but rather the lack of sufficient harmonisation within the EU of the rules concerning the processing of health data[6].

16. The EDPS would like to underline that guidance has already been provided on the application of the current data protection rules in the area of health, in particular by the Article 29 Working Party in its working document on the processing of personal data relating to health in electronic health records (EHR)[7], and by the Council of Europe[8]. The EDPS also has provided advice in connection with EU legislative proposals on health data and has highlighted in his Opinions how the relevant data protection principles under the current legal framework must be applied in that context[9]. The EDPS notes that the availability of such guidance in respect of eHealth processing operations taking place under the current legal framework has not been emphasised in the Communication with specific references to the relevant documents.

17. The EDPS welcomes, however, the clear link to the Staff Working Document on the applicability of the existing EU legal framework to telemedicine services, which contains useful information about the existing data protection legal framework and which was presented together with the Action plan.

2.3.2. Future guidance on the processing of Health data

18. The EDPS welcomes that the Commission will be preparing guidance on how the processing of health data should be done under the new data protection framework. In view of the challenges described in the data protection sub-section, such guidance should not only cover data portability and the right to be forgotten but also other challenging areas such as the concept of ownership of the data, the conditions of access and re-use of health data for research purposes, public health purposes, or possible additional purposes (such as current open data initiatives), or the use of cloud computing infrastructure and services for health and well-being data processing.

19. The EDPS believes that guidance would be particularly helpful on the issue of identifying who is the controller and on the responsibilities of the different operators involved in eHealth and well-being ICT, including of the designer of the ICT. He recommends that the Commission consults the Article 29

[6] See EDPS Opinion on the data protection reform package, para. 298 and 299, 7 March 2012, available at: www.edps.europa.eu.
[7] 15 February 2007.
[8] Recommendation No.R (97) 5 on the protection of medical data (13 February 1997).
[9] See in particular EDPS Opinion on the proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare, OJ C 128, 6.6.2009, p.20, EDPS Opinion on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health, 28 March 2012, EDPS Opinion on the proposal for a Regulation on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC and EDPS Opinion on the proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices, 8 February 2013 available at: www.edps.europa.eu.

Working Party, in which the EU national data protection authorities are represented, and the EDPS in the preparation of such guidance.

2.3.3. Design of eHealth and well-being ICT, medical devices and mobile applications

20. The EDPS welcomes that the Communication underlines that the design of eHealth and well-being ICT should implement the principle of privacy by design and by default and make use of Privacy Enhancing Technologies (PETs) as foreseen in the proposed data protection regulation and that the Communication makes reference to the principle that controllers shall be accountable for their data processing, carry out data protection impact assessments, and comply with strengthened security requirements.

21. The Communication makes a reference to the Commission proposals to strengthen the European regulatory framework for medical devices and in vitro medical devices. In this context, the EDPS would like to emphasise the data protection concerns highlighted in his recent Opinion on these proposals[10].

22. The use of m-health and health and well-being mobile apps poses considerable and new data protection challenges and must therefore also be analysed from a data protection perspective, with due account of the data protection legal framework and of the e-Privacy rules set forth in Directive 2002/58/EC[11]. Similarly to other forms of processing, general data protection principles are particularly relevant in the design and deployment of innovative mobile apps relating to health and well-being. In particular, the application of the principle of privacy by design and the use of PETs would allow data protection and privacy requirements to be embedded in such apps at the stage of their design.

23. For these reasons, the EDPS would like to be consulted before the adoption by the Commission of the planned Green paper on an EU framework applicable to m-health and health and well-being mobile apps.

2.4. Specific comments on other parts of the Action Plan

2.4.1. Supporting research, development and innovation in eHealth

24. In Section 5.1. of the Communication, it is stated that *'There will be an additional focus on ways of analysing and mining large amounts of data for the benefit of individual citizens, researchers, practitioners, businesses and decision makers.'* The EDPS notes that the Communication does not underline that any data mining is only acceptable in very limited circumstances and provided that full account is taken of data protection rules; he encourages the Commission to draw the attention of controllers to this fact.

[10] See EDPS Opinion on the proposals for a Regulation on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and a Regulation on in vitro diagnostic medical devices, 8 February 2013 available at: www.edps.europa.eu.

[11] For an analysis of the legal framework applicable to the processing of personal data in the distribution and usage of mobile apps, please see the recently published Opinion of the Article 29 Working Party on apps on smart devices, WP 29 Opinion 2/2013, WP 202 of 27.02. 2013.

25. To the greatest extent possible, any processing of large amounts of data for purposes of analysis should be done on the basis of anonymous data. In the context of health, the use of non-anonymous data may nonetheless be justified in certain cases for specific purposes (such as the study of epidemics, heredity, etc). However, the cases in which data mining may involve personal data and the extent of such personal data processing (e.g. the types of data processed) must be assessed on a case-by-case basis. Furthermore, the persons who are authorised to access these data and the modalities for such access should be clearly defined.

26. The defined standards and/or common guidelines to be developed in the context of pre-commercial procurement and public procurement of innovation should include rules on data handling including also safe deletion when data are no longer needed for the purposed envisaged.

2.4.2. Profiling

27. It is not clear what is meant under the objectives to have *'an ICT and computational science framework for digital, personalised and predictive medicine'*. To achieve such types of personalisation through ICT may require building up profiles of individuals on the basis of compiling data from different sources (e.g. user generated-data combined with health records). The combination of data for purpose of building up profiles raises serious data protection concerns, in particular if they lead to decisions being taken that may affect individuals (e.g. insurance companies may decide not to insure someone if they have access or require access to the health profile of an individual which shows predictions of a high probability of cancer). Hence, the EDPS notes that the Communication does not underline that profiling should only be done in very limited circumstances and provided that strict data protection requirements are met (e.g. as set forth in Article 20 of the proposed Data Protection Regulation) and recommends the Commission to remind controllers of this important obligation.

2.4.3. Facilitating wider deployment and supporting user skills and literacy

28. The EDPS welcomes the work planned by the Commission in supporting the work of the eHealth network, in defining a minimum dataset for health records, in providing guidance on electronic identification and authentication used in eHealth and in advancing the security and interoperability of databases for medicinal products. He wishes to underline that the work on all these topics should be done in accordance with data protection requirements. This was recognised explicitly in Article 14(2) last paragraph of Directive 2011/24 on the application of patients' rights in cross-border healthcare. Similarly, the EDPS recommends that the work of the Commission in these areas shall be pursued in due observance of the principles of data protection as set out, in particular, in Directives 95/46/EC and 2002/58/EC.

29. The EDPS also welcomes actions to promote skills and health literacy. He, however, would like to stress that the information to citizens on the benefits

and hazards of eHealth solutions should also include the required data protection information, including on how their data are processed and how they can control them. The EDPS therefore notes that the Communication does not include data protection as part of the promotion of skills and health literacy and recommends that the Commission considers data protection in any actions undertaken in this respect.

2.4.3. Fostering EU-wide standards, interoperability testing and certification of eHealth

30. There are many data protection risks to take into account for building up a common European eHealth Interoperability Framework (e.g. data quality and reliability, confidentiality, access restrictions, further use and purpose limitation principle, etc). Article 33 of the proposed Data Protection Regulation foresees for many processing operations, including for those on health data, that data protection impact assessments (DPIA) should be carried out before launching any interoperable system. The EDPS therefore recommends that the Commission carries out such a DPIA already today, before any further action is undertaken in this context.

31. The particular sensitivity of personal data concerning health and its protection under EU data protection legislation requires that the observation of data protection safeguards becomes an integral feature of the eHealth Interoperability Framework at all levels. Transfers of health data within and between jurisdictions must be executed in such a way that additional information required to respect purpose limitation and other constraints[12] on the processing of the data is transmitted together with the data in an interoperable format that both sender and receiver can understand.

32. The EDPS also urges the Commission, when examining the interoperability of health records, to look into possible legislative initiatives at EU level, as he believes that such interoperability would benefit from a strong legal basis, which would include specific data protection safeguards.

3. CONCLUSIONS

33. The EDPS welcomes the attention paid specifically to data protection in the proposed Communication, but identified some scope for further improvement.

34. The EDPS underlines that data protection requirements should be appropriately considered by industry, Member States and the Commission when implementing initiatives within the eHealth area. In particular he:

- emphasizes that personal data processed in the context of eHealth and well-being ICT often relate to health data, which require a higher level of data protection and underlines the guidance already given to controllers and processors in the area;

[12] This could indicate that if personal data concerning health is only allowed to be used for the treatment of the individual it relates to or if the patient has given his or her consent for some of the data to be used in a study or wider analysis.

- notes that the Communication does not refer to the current data protection legal framework set forth under Directive 95/46/EC and Directive 2002/58/EC, which contains the relevant data protection principles that are currently applicable and reminds the Commission that these rules are to be respected for any action to be taken in the short to medium term until the proposed revised Data Protection Regulation enters into force;

- notes that the importance of the data subject's rights of access and information in the context of eHealth has not been made clear in the Communication. He therefore encourages the Commission to draw the attention of controllers active in the field of eHealth on the necessity to provide clear information to individuals about the processing of their personal data in eHealth applications;

- notes that the availability of guidance in respect of eHealth processing operations taking place under the current legal framework has not been emphasized in the Communication with specific references to the relevant documents and recommends that the Commission consults the Article 29 Working Party, in which the EU national data protection authorities are represented, and the EDPS in the preparation of such guidance;

- recommends consulting the EDPS before the adoption by the Commission of a Green paper on an EU framework applicable to m-health and health and well-being mobile apps;

- notes that the Communication does not underline that any data mining using non-anonymous health data is only acceptable under very limited circumstances and provided that full account is taken of data protection rules and encourages the Commission to draw the attention of controllers to this fact;

- underlines that profiling should only be done in very limited circumstances and provided that strict data protection requirements must be met (e.g. as set forth in Article 20 of the proposed Data Protection Regulation) and encourages the Commission to remind controllers of this important obligation.

- reminds the Commission that any future work in the areas of facilitating wider deployment, supporting user skills and literacy should be pursued in due observance of the principles of data protection;

- recommends that the Commission carries out a data protection impact assessment in the context of the development of a common European eHealth Interoperability Framework, before any further action is undertaken;

- urges the Commission, when examining the interoperability of health records, to look into possible legislative initiatives at EU level, as he believes that such interoperability would benefit from a strong legal basis, which would include specific data protection safeguards.

Done in Brussels, 27 March 2013

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor