PURPOSE: For information to the eHealth WG
CONCERNING: Update
AUTHOR: CPME Secretariat

CPME REF NUMBER: CPME/2012/063
DATE: 13 April 2012
CONFIDENTIAL

Commission Draft Regulation on Data Protection - Analysis
13 April 2012

***Printing notice: please note that the document exceeds 10 pages

Table of Contents

PURPOSE: For information to the eHealth WG
CONCERNING: Update
AUTHOR: CPME Secretariat

CPME REF NUMBER: CPME/2012/063
DATE: 13 April 2012
CONFIDENTIAL

I. INTRODUCTION

1. Review EU legal framework on data protection

The legal framework regarding the protection of personal data (mainly established by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data – hereinafter: "Directive") is currently being reviewed by the European Commission (hereinafter: "EC").

i. Purpose of review:

a) Adapt existing data protection legislation to respond to (1) rapid development of new technologies, and (2) increasing globalisation; and
b) Ensure free data flow on the EU single market and reduce administrative burden of companies by harmonizing data protection legislation in the EU.

ii. Legislative process:

a) First initiative for the review launched by the EC in May 2009.
b) Organisation of public consultation (i.e. July - December 2009 and November 2010 – January 2011) and discussions with stakeholders.
c) Resulted in a legislative proposal to reform Directive on January 25, 2012.
d) EC proposes replacing the Directive by (1) a General Data Protection Regulation (hereinafter: "Regulation); and (2) a Directive regarding processing of personal data performed by competent authorities for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
e) The current legislative proposal is still being discussed and final adoption of the Regulation can take up to two years.
f) After adaption, the Regulation will enter into force the 20th day following the publication in the Official Journal of the European Union (art. 91).
g) The Regulation shall apply as from two years from the entry into force (art. 91).

iii. Why a regulation instead of a directive?

a) A directive requires implementation in national legislation (except in case of late or incorrect implementation).
b) A regulation is directly applicable in EU member states.
c) Directives allow EU member states to implement the rules with a certain flexibility. However, this leads to the current lack of harmonisation of data protection rules in the EU and legal uncertainty which is one of the main reasons for the current review.
d) Therefore, the EC proposes to replace the Directive by the Regulation, which is expected to provide a harmonized legal framework for data protection in the EU.

iv. Consequences of the choice for a regulation:

a) Direct applicability in member states with limited implementations into national law. This ensures a harmonised legal framework and legal certainty regarding data protection requirements.
b) EC has delegated powers to adopt acts to further specify certain provisions in the future. This entails that the provisions in the Regulation only form a basic framework which can be further developed by the EC. Therefore, it would be difficult for companies to anticipate further developments of the data protection legislation.

II. COMPARISON WITH CURRENT DIRECTIVE AND IMPLICATIONS FOR CPME MEMBERS

1. Territorial scope of the Regulation (Art. 3)

i. Proposed regime:

The draft Regulation will apply to processing of personal data performed in the context of the activities of an establishment of a controller (e.g. a physician) or a processor (e.g. a physician) in the EU.

2. Material scope of the Regulation: The concept 'data subject' and "personal data"(Art. 4.1)

i. Proposed regime:

The Regulation defines the concept "data subject" as:

"an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

ii. Comparison with the existing Directive:

The definition specifically mentions identification of individuals by reference to:

- location data;
- online identifiers; and
- genetic data.

iii. Considerations for CPME Members:

The processing of genetic data triggers the sensitive data processing regime which may be further regulated by the EC through secondary regulations (Art. 9(3) Regulation). In addition, such data processing is considered to constitute a high privacy risk which requires that a privacy impact assessment be made prior to processing (Art. 33 Regulation).

3. **The data subject's consent (Art. 4.8)**

i. Proposed regime:

The Regulation defines the data subject's consent as:

"*Any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".*

ii. Comparison with the existing Directive:

The requirements for valid consent are stricter than under the current Directive:

a) The definition requires that consent is given explicitly, either by a statement or by a clear affirmative action (i.e. opt-in).

→ Directive: explicit consent is only required for sensitive data processing. In other cases, unambiguous consent (which can be implicit) is sufficient.

b) The Regulation contains addtional conditions for consent (Art. 7):

→ If consent is obtained through a written declaration, which also concerns another matter (such as general terms of use), the consent must be presented seperately;

→ If there is a significant imbalance between the position of the data subject and the controller (e.g. in an employee-employer relationship) it is not possible to rely on consent.

4. **Specific provision regarding health**

i. Proposed regime:

a) Definition of health data (art. 4.12):

Health data is "*any information which relates to the physical or mental health of an individual, or the provision of health services to the individual*".

b) Principle (art. 9 (h)):

Processing health data is permitted if necessary for health purposes under certain conditions (included in Art. 81).

c) Specific conditions (art. 81):

Health data processing is permitted if necessary for:

a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person subject to an equivalent obligation of confidentiality; or
b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or
c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.
d)

ii. Comparison with the existing Directive:

Processing of health data is subject to the general restrictions on the processing of sensitive data. One specific exemption was provided: Health data processing by healthcare professionals (or other persons subject to professional secrecy obligation) required for the purpose of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, is permitted.

iii. Considerations for CPME Members:

Note that the EC has been provided with delegated powers to adopt secondary legislation which may further specifies the processing conditions of health data (Art. 81 (3)).

5. **Specific provision for scientific research (art. 83)**

i. Proposed regime:

a) Principle:

Processing (health) data for historical, statistical or scientific research purposes (such as for improving diagnoses, preparing studies for therapies etc.) is only permitted under the conditions included in art. 83.

a) Specific conditions (Art. 83):

Processing of personal data for historical, statistical or scientific research is permitted if:

1) the purpose cannot be otherwise fulfilled by processing data which does not permit the identification of the data subject; and
2) data enabling the attribuation of information to an identified or identifiable data subject is kept seperately from the other information as long as the purposes can be fulfilled in this manner.

6. **Data subject's rights**

i. Proposed Regime:

A) Requirements for handling data subjects' requests:

Data controllers (e.g. physicians) will be required to:

a) implement procedures for providing information and enabling data subjects to exercise their rights.
b) inform data subjects within 1 month of the actions taken following their request.
c) provide information in writing or in electronic form if the request was made electronically.

In case the requested action is refused, the data subject must be informed of (a) the reasons for refusal, and (b) his/her option to lodge a complaint with the Data Protection Authority (hereinafter: "DPA") or relevant court.

Information and exercise of the data subjects' rights must be free of charge (unless in case of manifestly excessive requests).

B) Notice requirement (art. 14):

In addition to the information required under the Directive, the following information must be provided to the data subject:

a) Contract terms and conditions in case processing is necessary to perform a contract;
b) Legitimate interest of controller in case processing is based on this ground;
c) Retention period;
d) Right to lodge a complaint to the DPA and its contact details;
e) Information regarding international data transfers and level of data protection in the country of destination by reference to an adequacy decision by the EC; and
f) The source of personal data in case it is not collected directly from the data subject.

C) Right to be forgotten (art. 17):

a) Principle:

The data subject has the right to demand the erasure and prevent further dissemination of his/her personal data, in case:

1) it is no longer necessary to achieve the purpose for which they were collected;
2) he/she withdraws his/her consent or the period for which this consent is given expired and there is no other justification ground; or
3) personal data is processed in violation of the Regulation.

b) Notification of data recipients:

In case personal data is made public to other parties, it is required to take all reasonable steps to inform these third parties that they must erase any link to the personal data and erase each copy or replication of the personal data.

c) Restrictions on the right to be forgotten:

Erasure of data is not required if the retention is necessary:

1) to exercise the right of freedom of expression (as defined in Art. 80 Regulation);
2) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety for medical products or medical devices;
3) for historical, scientific or statistical research; or
4) to comply with a legal obligation to retain personal data of the EU, or a member state.

D) Right of Access and Amendment (Arts. 15-16):

Data subjects have the right to access personal data concerning them. Furthermore, data subjects have the right to demand rectification of inaccurate or incomplete data. Specifically, the following information must be provided further to a valid request:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data are to be or have been disclosed, in particular to recipients in third countries;
- the period for which the personal data will be stored;
- the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;
- the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; and
- communication of the personal data undergoing processing and of any available information as to their source.

ii. Comparison with existing Directive:

The Regulation will strengthen the data subjects ability to control personal data by providing the data subject with more rights and improved means to exercise these rights.

In this sense, the Regulation contains (a) additional requirements for handling requests of data subjects; (b) broader notice requirement; (c) a new right to be forgotten and right to data portability; and (e) a clearer right to object.

iii. Considerations for CPME Members:

Medical practices will have to implement procedures to be able to respond and handle requests of data subjects in compliance with the Regulation. Furthermore, notice forms will need to be amended to include the required additional information.

iv. Considerations for CPME Members:

Medical practices will have to implement procedures to be able to respond and handle requests of data subjects in compliance with the Regulation. Furthermore, notice forms will need to be amended to include the required additional information.

7. **Accountability of data controller**

i. Proposed regime:

A. Requirement to implement data protection procedures and policies:

It is required to implement policies and measures to ensure and to demonstrate that processing is performed in compliance with the Regulation.

→ Accountability idea: the data controller must be able to show that the processing is legitimate (replaces registration obligation with the DPA).

B. Requirement to keep documentation (Art. 28 Regulation):

a) General obligation:

It is required to keep records with at least the following information:

1. Name and contact details of the controller, joint controller or processor;
2. Name and contact details data protection officer (hereinafter: "DPO");
3. Purposes (including legitimate interests if relevant);
4. Description of data categories and data subjects;

5. Categories of recipients;
6. International transfers (and if relevant documentation on appropriate safeguards for adequate protection);
7. Retention periods; and
8. Documentation on mechanisms to verify effectiveness of data protection measures.

b) Exemptions:

The documentation requirement does not apply to:

1. Individuals processing data without commercial interest; and
2. Enterprises or organizations with less than 250 employees processing personal data as an activity ancillary to its main activities.

C. Data Protection Impact Assessment (Art. 33 Regulation):

a) Principle:

In certain cases it is required to perform a Data Protection Impact Assessment prior to commencing the processing.

b) When?

Only required for certain types of processing, presenting specific risks:

1. Profiling;
2. Processing of sensitive data or processing to provide health care, epidemiological researches, or surveys of mental or infectious diseases, when performed to take measures or decision regarding specific individuals on a large scale;
3. Surveillance in public areas;
4. Processing of data regarding children, genetic or biometric data in large scale filing systems; and
5. Processing which requires consultation of the DPA.

c) Elements of Data Protection Impact Assessment:

The Data Protection Impact Assessment must include the following elements:

1. Description of processing;
2. Assessment of risks for rights of data subjects;
3. Measures to address risks;
4. Safeguards, security measures and mechanisms to protect personal data; and

5. View of the data subjects or their representatives on intended processing.

d) Consequences:

In case the Data Protection Impact Assessment determines that there is a high degree of specific risks, consultation of the DPA would be required. Please note that not performing the obligatory Data Protection Impact Assessment could be sanctioned by the DPA with an administrative fine of up to 2% of the annual worldwide turnover of the company (!).

8. Enforcement of the Regulation (Art. 73 – 79 Regulation)

i. Proposed regime:

The Regulation would provide several mechanisms to enforce its application:

a) Complaint with DPA:

Data subjects have the right to lodge a complaint with the DPA. Furthermore, organizations, bodies or associations which aim at protecting data subjects' rights (such as consumers organizations), also have the right to lodge a complaint with the DPA on behalf of a data subject.

→ The data subjects have the right to a judicial remedy against the decisions of the DPA or to oblige the DPA to act on a complaint in the absence of a decision within three months.

b) Judicial remedy:

Data subjects have the right to a judicial remedy against the data controller or processor in case their rights under the Regulation have been infringed.

→ This right may be exercised on behalf of one or more data subjects by organizations aiming at protecting data subjects' rights.

c) Right to compensation:

Data subjects have the right to receive compensation of the data controller or processor for damages resulting from unlawful or incompliant processing of their personal data.

→ Data controller or processor will be exempted from liability in case he proves that he is not responsible for the event causing the damage.

→ In case several controllers or processors are involved, each of them is responsible for the entire amount of the damage.

d) Legal penalties:

EU member states are required to provide effective, proportionate and dissuasive penalties for violations of the Regulation.

e) Administrative sanctions:

- DPAs can impose effective, proportionate and dissuasive administrative sanctions on data controllers or processors.
- These sanctions will vary taking into account the nature, gravity and duration of the violation, the degree of responsibility, previous violations, co-operation with DPA and implemented measures and procedures.
- Maximum fine of up to 2% of the annual worldwide turnover of the company.

***