Directive 95/46 and the use of GRID technologies in the healthcare sector: selected egal issues[4]

Jean A.M. HERVEG & Yves POULLET

Centre de Recherches Informatique & Droit
Faculté de Droit de Namur – FUNDP - Belgique

Running Title: Legal issues for the use of GRID in the healthcare sector

Corresponding Author: Jean A.M. HERVEG, Centre de Recherches Informatique & Droit, A l'attention de M. Jean A.M. HERVEG, 5 rempart de la Vierge, B – 5000 NAMUR, Belgium

---

Abstract. Directive 95/46 prescribes rules concerning data processing that have to be implemented by each Member State in order to protect the data subject's privacy and to ensure the free movement of personal data within Europe. The data processing includes all operations linked to the same purpose and performed upon patient's data when using Health Grid services. As a result of the implementation of this Directive, the data processing must be legitimate and comply with standards of data quality. The confidentiality and security of the data processing have to be enforced. The controller has to notify the data processing to his supervisory authority prior to carry it out. The data subject has a right to be informed about the data processing, to access his/her personal data, and to object to the processing under particular circumstances. In case of violation of his/her rights, the data subject has a right to judicial remedies and to receive compensation.

Key words: Grid technologies, HealthCare Sector, Legal Aspects, Directive 95/46, Processing of personal data

---

1. Introduction

The use of Grid technologies in the HealthCare Sector implies automated processing of personal data concerning the patient's health, for therapeutic and scientific purposes. In this

---

(4) This work was supported by the EC under Research Contract IST-2001-37153 GEMSS (GRID enabled Medical Simulation Services).

context, end-users will collect and dispatch the patient's personal data to Health Grid Services Providers. These providers will process the patient's personal data in order to complete the therapeutic or scientific purpose on behalf of the end-users, before sending them back or making them available to the end-users if needed.

Directive 95/46([5]) prescribes rules concerning the processing of personal data that have to be implemented by each Member State in order to protect data subject's privacy (art. 1, 1) and to ensure the free movement of personal data within Europe ([6]) (art. 1, 2).

This paper aims to introduce in a few words some relevant provisions from Directive 95/46 with regard to the use of Grid technologies in the HealthCare Sector (IV-VII). Prior to do so, it seems useful to remind a few legal definitions stated by this Directive (I) and to define its scope (II) as well as the applicable National law (III).

2. Legal definitions stated by Directive 95/46 (art. 2)

1. Personal data (art. 2, a)

Personal data mean any information relating to an identified or identifiable natural person (the data subject). An identifiable person is one which can be identified, directly or indirectly, in particular by reference to an identification number (e.g. a code) or to one or more factors to one's physical, physiological, mental, economic, cultural or social identity.

2. The processing of personal data (art. 2, b)

The processing of personal data is constituted from any operation or set of operations linked to the same purpose and which are performed upon personal data, whether or not by automatic means. The processing of personal data is defined by the goal pursued by the controller. There are as much different data processing as there are different purposes. Operations include e.g. collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

3. The controller of the data processing (art. 2, d)

([5]) D., 95/46/CE 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. Official Journal L 281, 23/11/1995:0031-0050.

([6]) BOULANGER M-H, de TERWANGNE C, LEONARD Th, LOUVEAUX S, MOREAU D, POULLET Y. La protection des données à caractère personnel en droit communautaire. JTDE 1997 : 145-155 et 173-179.

The controller is the natural or legal person, public authority, agency or any other body which alone or with others determine the *purposes* and *means* of the data processing. He has to ensure the compliance of the data processing with the national law transposing EU Directive 95/46.

4. The processor of the data processing (art. 2, e)

The processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

3. Scope of Directive 95/46 (art. 3)

Directive 95/46 applies to the wholly or partly automated processing of personal data, and to the processing of personal data realized otherwise than by automatic means but which form part of a filling system or are intended to form part of a filing system (art. 3, 1).

Directive 95/46 shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law ([7]), such as those provided for by Titles V (Provisions on a common foreign and security policy) and VI (Provisions on police and judicial cooperation in criminal matters) of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law (art. 3, 2).

Directive 95/46 shall no more apply to the processing of personal data by a natural person in the course of a purely personal or household activity (art. 3, 2).

4. National law applicable to the processing of personal data (art. 4)

The national provisions adopted by a Member State pursuant Directive 95/46 shall apply to the processing of personal data carried out in the context of the activities of an establishment of the controller on the territory of the Member State.

If the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the applicable national law.

([7]) About Directive 95/46's scope, cf. : Opinion of the Advocate General M. ANTONIO TIZZANO at the sitting on 19 September 2002, in case C-101/01, Bodil Lindqvist v. Åklagarkammaren i Jönköping (for a preliminary ruling in the proceedings pending before Göta hovrätt).

The national provisions adopted by a Member State pursuant Directive 95/46 shall apply to the processing of personal data where the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law.

The national provisions adopted by a Member State pursuant Directive 95/46 shall apply to the processing of personal data where the controller is not established on Community territory but, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

5. General rules of lawfulness to be implemented by EU Member States with regard to the processing of personal data (art. 5-21)

Member States shall, within the limits of the provisions of Directive 95/46, Chapter II, determine more precisely the conditions under which the processing of personal data is lawful (art. 5).

A. <u>Principles relating to data quality</u> (art. 6)

1° Personal data must be processed *fairly* and *lawfully*. The data processing has to be transparent and fulfill all special rules applicable to the processing of personal data concerning health, such as e.g. medical secrecy rules.

2° Personal data must be collected *for specified, explicit and legitimate purposes* and cannot be further processed in a way incompatible with those purposes. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that applicable national law provides appropriate safeguards.

3° Personal data must be *accurate* and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data, which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.

4° Personal data must be kept in a form which permits identification of data subjects *for no longer* than is necessary for the purposes for which the data were collected or for which they are further processed (e.g. therapeutic and scientific purposes but also keeping records for liability reasons).

B. <u>Criteria for making data processing legitimate</u> (art. 7)

The processing of personal data must comply with the criteria selected by the applicable national law for making the data processing *legitimate*. By way of example, the legitimate character might result from the unambiguously consent of the data subject or from the legitimate interests pursued by the controller, or when the processing is necessary in order to protect the vital interests of the data subject (e.g. emergency cases). But the data processing should not be considered as legitimate where the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, are overridden by the interests for fundamental rights and freedom of the data subject which require protection under Article 1 of the Directive 95/46. *As a result, the legitimate character of the data processing must be effectively assessed in each case.*

C. Special categories of data processing (art. 8-9)

Member States shall prohibit the processing of personal data *concerning health* excepted e.g. where it is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, etc. However, there is no specific exception here for scientific purposes. Directive 95/46 only adds that Member States may lay down, with suitable safeguards, additional exemptions for reasons of substantial public interests. That should allow exemptions e.g. for scientific purposes.

The personal data concerning health must be processed *by a health professional* subject under national law or rules established by national bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

The applicable national law should determine the conditions under which a national identification number or any other identifier of general application may be processed (e.g. for patient's identification). It is recommended to assign a *specific identification number* to the patient in case of processing of personal data concerning health and to avoid using social security numbers or any other number used for administrative purpose or for any other non-health related purposes.

D. Data subjects' rights (art. 10-15)

1° Information to be given to the data subject (art. 10-11-13)

The controller or his representative must provide the data subject from whom data relating to himself are collected with at least some *information*, e.g. the controller's identity, the purposes of the data processing, the recipients or categories of recipients of the processed data, the existence of the right to access and the right to rectify the data, etc.

2° Right of access to personal data (art. 12-13)

The data subject has the right to obtain from the controller communication in an intelligent form of the data undergoing processing, and of any available information as to their sources.

3° Right to object to the data processing (art. 14)

The data subject has the right to object at any time on compelling legitimate grounds relating to his/her particular situation to the processing of data relating to him/her, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve such data.

E. Confidentiality of personal data processing (art. 16)

In order to ensure data processing's *confidentiality*, any person acting under the authority of the controller, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.

F. Security of personal data processing (art. 17)

The controller must implement *appropriate technical and organizational measures* to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. With regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. With respect to this, it is useful to refer to REC 1997(5) of 13 February 1997 of the Council of Europe on the protection of medical data (art. 9) and to REC 1983 (10) of 23 September 1983 on the protection of personal data used for scientific research and statistics (art. 7).

If the processing is carried out on his behalf, the controller has to choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

Carrying-out the processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that (1) the processor shall act only on instructions from the controller and that (2) the appropriate technical and organizational measures set out in article 17, § 1, of Directive 95/46, shall also be incumbent on the processor.

In view of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in article 17, § 1, of Directive 95/46, shall be in written form or another equivalent form.

G. Notification of data processing to the supervisory authority (art. 18-19)

The controller must notify the competent supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

6. Judicial remedies and liability rules to be implemented by EU Member States (art. 22-23-24)

Every person has the right to a judicial remedy for any breach of the rights guaranteed by the national law applicable to the processing in question.

Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to Directive 95/46 is entitled to receive compensation from the controller for the suffered damage. The controller might be exempted from this liability in whole or in part if he proves that he is not responsible for the event causing the damage.

7. Transfer of personal data to Third Countries (art. 25-26)

Member States shall provide that the transfer to a third country of personal data, which are undergoing processing or are intended for processing after transfer, may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of Directive 95/46, the considered third country ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all circumstances surrounding a data transfer operation or set of data transfer operations. The EU Commission may find that a third country does or does not ensure an adequate level of protection. There might be data transfer to third country with no adequate level of protection in several cases e.g. if the data subject has consented unambiguously to the proposed transfer ([8]).

([8]) HAVELANGE B, LACOSTE AC. Les flux transfrontaliers de données à caractère personnel en droit européen. JTDE 2001 :241-248 ; HUART S, Les « Safe Harbor Principles » ou « Les Principes de la Sphère de Sécurité ». DA/OR Act. 2000-01;4:14-16

8. Codes of conduct (art. 27)

Member States and EU Commission shall encourage the drawing-up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to Directive 95/46, taking into account the specific features of the various sectors.

9. Conclusions

Directive 95/46 concerns Health Grid Services where their use implies processing of personal data. In this case, the controller has to ensure the lawfulness of the data processing including confidentiality and security of the data processing as well as the implementation of the data subject's rights. One task for a Health Grid Cluster could be to draw up a code of conduct for Health Grid Services in Europe.