Rules and Regulations for the Establishment of a Biometric Database Among European Member States

By Anne-Gaëlle LEFEBVRE

To BioSecure Association

Table of contents

Preface :

A major integrative effort within the BioSecure Network of Excellence lies with the design and collection of a new multimodal database. It will take place in the second part of the project (i.e. second 18 months). This database will allow for the creation of a common and repeatable benchmark of algorithms. Several partners will be involved in the acquisition of the BioSecure Multimodal Biometric Database.

Legal aspects have to be handled when performing acquisition, storage and exchange of biometric data. When defining a biometric database, specific issues have to be tackled before the acquisition process itself can begin. Indeed particular aspects related to the protection of personal data as well as the rights of the persons regarding data stored in centralised databases have to be addressed. There is a variety of restrictions, which are dependent to a certain extent on the different national legislations. To take into account this legal side, the regulations are being studied in the context of multi-national and multi-modal biometric data acquisition under consideration of national conditions. Other issues related to IPRs are also being studied.

In the following section, legal requirements related to the BioSecure Multimodal Biometric Database are discussed, including Data Protection issues and IPRs issues. Agreement with 'donors', control and processing of the data and transfer of data between institutions are specifically addressed.

While there has been a harmonization of the basic requirements for data protection at the EU level, differences remain as to the administrative steps required and as to non-EU legislations.

Now biometric data are considered as sensitive data and go into the field of application of the personal data protection. The first convention who is taking rules of data protection is the 108 convention of European council at 28 January 1981[1].

The definition of personal data is given by the European directive of 1995[2] and repeated in European country law: "personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); 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".

There are the cases of biometric data, because they allow directly and indirectly the identification of a person and are thus protected as some. More, this data are considered by The European commission as sensitive data. Her protection is stricter.

The establishment of a personal data processing is subject to certain formalities and procedures.

---

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm

[2] 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

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

➢ Legal requirements

• Applicable law

The law of which country applies? Which data commissioner is competent? The answer depends on which institute is responsible for the data processing activity:

- Institutes with establishment in an EU member state: for *data processing* in another EU country, the law of the country where the *responsible party* for the data collection is established; for *data processing* in a non-EU country, the law of the country where the activity takes place.

- Institutes established in non-EU countries: the law of the country where the *data processing* takes place.

• Quality of data:

Article 6 of the European Directive of 1995 lays down the conditions under which the retained data must meet. These conditions are related to their collection should be fair and lawful, but also with a defined and legitimate purpose.

"(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) 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;

(e) 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. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. »

- **Principles surrounding the introduction**

  - General cases

A system of automated data processing must be legitimate in its implementation. Restrictive cases provided for in Article 7 of the European directive of 1995:

"a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1). »

  - The authorization of the data subject:

One of the easiest conditions to be fulfilled is to have the authorization of the data subject because Biometric data are sensitive data. This authorization is valid if it must be contain the conditions of any contract. Indeed, the person must give its consent in full knowledge and acceptance must be explicit and not assumed. The lack of rejection of non-collection is not enough. The data subject must have the possibility to withdraw this consent at any time.

The permission should specify the purpose of data collection, the kind of use envisaged and possible transfers to other legal entities that guarantee the same level of protection as the Institute collecting the data.

  - Information to be transmitted to people involved:

There are obligations in terms of informing the data subject which are under the responsibility of the data processing controller. These are set out in Article 10 of the European Directive of 1995.

The main information that must be transmitted to the data subject is the identity of the controller. There is contact information the data subject can use to contact him to exercise its right to access, correct or delete their personal data for example.

The person must also be informed in case of data transfer to a state not a member of the European community.

➢ National data commissioner

All EU countries have a national data commissioner, who controls the compliance with the data protection laws (e.g. CNIL in France). Most EU legislations require a (prior) declaration of data processing activities with the data commissioner, details vary. Some general rules are given below.

In order to be getting a more complete picture of the country specific requirements, all partners involved in the acquisition are asked to contact the data commissioners of their country for the requirements that apply for data registration, use and transfer. The objective is to get a complete picture of the requirements and constraints before data acquisition activities are launched.

Country	National data commissioner
Germany	Der Bundesbeauftragte für den Datenschutz (Federal autority) Husarenstraße 30 53117 Bonn GERMANY website : www.datenschutz.de
austria	Direktor Buro der Datenschutzkommission und des Datenschutzrater Bundeskanzlerant Ballhausplatz 1 1014 Vienne AUSTRIA website : www.bka.gv.at/datenschutz
belgium	Commission pour la protection de la vie privée Rue Haute, 139 B-1000 Bruxelles BELGIUM Site web : http://www.privacy.fgov.be/
bulgaria	Bulgarian Commission for Personal Data Protection 1 Dondikov Blvd. 1000 SOFIA BULGARIA Site Web : http://www.cpdp.bg/en_index.html
Cyprus	Commission for Personal Data Protection 40 Th Dervis Street 1066 NICOSIA CYPRUS Site Web : www.dataprotection.gov.cy
Denmark	Datatilsynet Christians Brygge 28 4 sal 1559 Copenhague DENMARK Site web : www.datatilsynet.dk
Spain	Agencia de Protection de Datos C/ Jorge Juan, 6 28001-Madrid SPAIN Site web : www.agpd.es

Estonia	Estonian Data Protection Inspectorate Väike-Ameerika 19 10129 Tallinn ESTONIA Site Web : http://www.dp.gov.ee/index.php?id=14
Finland	Office of the Data Protection Ombudsman Albertinkatu 25 PO Box 315 00181 Helsinki FINLAND Site web : www.tietosuoja.fi/index.htm
France	Commission nationale de l'informatique et des libertés 8, rue Vivienne CS 30223 FRANCE F-75083 Paris Cedex 02 Site web : www.cnil.fr
Greece	Hellenic Data Protection Authority Kifisias Avenue 1-3 PC 115 23 Ampelokipi Athènes GREECE Site web : www.dpa.gr
Hungary	Parliamentary commissioner for data protection and freedom of information Nádor u. 22. 1051 Budapest HUNGARY Site web : www.obh.hu
Ireland	Data protection commissioner Block 4, Irish Life Centre Talbot Street - Dublin 1 IRLAND Site web : www.dataprivacy.ie
Italy	Garante per la protezione dei dati personali Piazza di Monte Citorio n.121 00186 Rome ITALY Site web : www.garanteprivacy.it/
Latvia	Data State Inspection Kr. Barona Street 5-4 1050 Riga LATVIA Site Web : www.dvi.gov.lv/
Lithuania	State Data Protection Inspectorate Gedimino ave.27/2 LT - 2600 Vilnius LITHUANIA Site Web : www.is.lt/dsinsp

Luxembourg	Commission nationale pour la protection des données 68, rue de Luxembourg 4221 Esch-sur-Alzette LUXEMBOURG Site web : http://www.cnpd.lu/
Malta	Office of the Commissioner for Data Protection Commissioner for Data Protection 280, Republic Street Valletta GPO 01 MALTA Site Web : www.dataprotection.gov.mt
Netherlands	Dutch Data Protection Authority PO Box 93374 2509 AJ. The Hague NETHERLANDS Site web : www.cbpweb.nl
Poland	Biuro Geneeralnego Inspektora ul. Stawki 2 0193 Warsaw POLAND Site web : www.giodo.gov.pl
Portugal	Comissào Nacional de Potecçào de Dados Informatizados 148, rue de Sao Bento 1200 Lisbonne PORTUGAL Site web : www.cnpd.pt
Czech Republic	Office for Personal Data Protection Pplk. Sochora 27 170 00 Prague 7 CZECH REPUBLIC Site web : www.uoou.cz
Romania	The National Supervisory Authority for Personal Data Processing 32, Olari Street Bucharest - Sector 2 ROMANIA Site Web : www.dataprotection.ro
United Kingdom	The office of information Commissioner Wycliffe House - Water Lane Wilmslow - Cheshire SK9 5AF UNITED KINGDOWN Site web : www.dataprotection.gov.uk
Slovak Republic	Office for the Protection of Personal Data Odborárske nám. 3 817 60, Bratislava SLOVAK REPUBLIC Site web : www.dataprotection.gov.sk

Slovenia	Namestnik varuha clovekovih pravic Urad varuha clovekovih pravic Dunajska 56 1000 Ljubljana SLOVENIA Site Web : http://www.ip-rs.si/
Sweden	Datainspektionen Box 8114 104 20 Stockholm SWEDEN Site web : www.datainspektionen.se

➢ Method of exercising the right of access to data subject

The data subject can exercise several rights. The first is the right to object: in fact each person is able "to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him". This right is provided in article 14 of the European directive of 1995.

Data subject have a right of access to these data. The details of this right of access are laid down in Article 12 of the European Directive of 1995:

"Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) Without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort. »

➢ Transfer of the biometric database to other countries

• toward European Union member states and European Economic Area

No formalities are necessary to transfer personal data to these countries. In otherwise, we must add the countries of the European Economic Area which have also transposed the European directive of 1995 into their national legislation, and adopting a level of protection of personal data equal to the European Union member states.

• toward Switzerland, Canada, Argentina, Jersey, Guernsey and the Isle of Man

The transfer of a database to the countries listed above no formalities. These countries were considered by the European Commission as having an adequate level of data protection because they have adopted data protection act or privacy act, even if they do not the exact words of the European Directive. These countries have also established a national data commissioner as the CNIL in France. Normally the transfer is not subject to any formality except perhaps a notification to the national data commissioner.

• toward the United States subject to adherence to the “Safe Harbor privacy principles "

The transfer to the united-state is particular. An agreement was signed between US government and the European Commission to the establishment of a "safe harbor" to encourage the transfer of personal data from Europe to the United States.

These principles are directly inspired from the 1995 directive, and contain basic principles, such as informing people, the possibility for the data subject to object to the transfer to third parties or use data for different purposes, explicit consent for sensitive data, access or security of the transfer itself.

It is a decision of the European Commission dated 26 July 2000 which gives the equivalent level of protection to companies adhering to the Safe Harbor. This safe harbor includes "safe harbor privacy principles but also the FAQ (15).

The approach for companies who want to are simple because they are enough to write a letter informing the US Department of Commerce that the company joined the Safe Harbor. It must publicly declare its adherence to the "safe harbor". It must also be under the jurisdiction of the Federal Trade Commission.

« safe harbor privacy principles [3]» and FAQ[4] are in the Us department of commerce website[5] .

[3] http://www.export.gov/safeharbor/eg_main_018247.asp

[4] http://www.export.gov/safeharbor/eg_main_018237.asp

[5] http://www.export.gov/safeharbor/

- **toward third countries outside the European Union and not have an sufficient level of protection**

  - creation of a contract to cross-border flow data

The realization of a border flow contract of data is a previous for transfer. It aims to level the lack of legislation in the country. It must be transmitted to the national data commissioner. In most European member state, the data transfer requires the authorization of the national data commissioner.

  - use of standard contractual clauses

The European Commission has established the standard contractual clauses which comply with the requirements of European legislation. They are available in all European languages. They are available in two versions, one dating from 2001[6] and another in 2004[7].

The all national data commissioner considers that clauses conferred an adequate protection in ad equation with the European Union law.

Some additional clauses may be added. However they do not reduce the level of protection afforded to data otherwise the transfer will be refused by the national data commissioner.

  - The preliminary information of the data subject

Data subject must be informed before any transfer of the data base to countries which do not receive adequate protection.

[6] English version Of contractual clause of 2001 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF

[7] English version of contractual clause of 2004 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF

- **exceptions allowing the transfer to a third country does not ensure an adequate level of protection**

There are derogations pursuant to Article 26-1 of the European directive of 1995:

“1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.”

The Article 29 group, recommends "that repetitive, mass or structural data transfers, the importance of regularity or warrant that they are framed in a precise manner, subject to specific legal and not based therefore not on such exceptions. "

In summary, the use of these exemptions should be that alternative; the controller should emphasize the establishment of rules or contract establishing an adequate level of protection.

The need for a strict interpretation is consistent with the recommendations adopted by the Working Group on Article 29 in its working document WP 12[8].

[8] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf