# BIOVISION

**Privacy Best Practices in Deployment of Biometric Systems**

---

<table>
<thead>
<tr>
<th>Project Number</th>
<th>IST-2001-38236</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Title</td>
<td>BIOVISION</td>
</tr>
<tr>
<td></td>
<td>Roadmap to Successful Deployments from the User and System Integrator Perspective</td>
</tr>
<tr>
<td>Deliverable Type</td>
<td>Document</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deliverable Number</th>
<th>BIOVISION: D7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractual date of delivery to Commission</td>
<td>31 July 2003</td>
</tr>
<tr>
<td>Actual date of delivery to Commission</td>
<td>28 August 2003</td>
</tr>
<tr>
<td>Title of the Deliverable</td>
<td>Final Report</td>
</tr>
<tr>
<td>Workpackage contributing to the Deliverable</td>
<td>WP 7</td>
</tr>
<tr>
<td>Author</td>
<td>Astrid Albrecht (Head of TeleTrusT Working Group Biometrics, Germany)</td>
</tr>
</tbody>
</table>

### Abstract:

This is Issue 1 of the Best Practices in the deployment of biometric systems. It focuses on legal and operational aspects relating to privacy.
About this document

Any enquiries about this document should be directed to:

Dr. jur. Astrid Albrecht  
Head of TeleTrusT Working Group 6 Biometrics  
TeleTrusT Deutschland e.V.  
Chamissosstrasse 11  
99096 Erfurt  
Germany  
http://www.teletrust.de  
E-mail: AAlbrechtLaw@aol.com

With contributions from:

Steffan Wettig  
Ref. iur.  
Friedrich-Schiller-Universität Jena  
Fakultät für Mathematik und Informatik  
Institut für Informatik  
Ernst-Abbe-Platz 1-4  
D-07743 Jena  
Germany


Disclaimer

The information in this document is provided on an 'as is' basis, with no guarantee or warranty given or implied that the information is fit for a specific purpose. Users make use of any material at their own risk and liability; and it is strongly recommended that these resources should be used only as guidelines in the formation of an overall strategy. The views expressed are those of the authors and do not necessarily reflect those of the European Commission. All trademarks are acknowledged.

Copyright

Copyright © Dr. Astrid Albrecht

This document may not be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without a prior written permission of the author. If granted, the acknowledgement of the author of the document must be clearly referenced.
Introduction

I Context

Although it is widely acknowledged that the addressing of privacy concerns is a major factor in the deployment of services using biometrics, there still exists a lot of confusion, uncertainty and even ignorance within the biometrics community and among public opinion of the privacy impacts biometrics can have and the corresponding obligations mainly on the part of the system integrators, Governments those procuring biometric systems and the operators.

Biometrics as discussed herein are those that can be categorised as mainly *automated* authentication which are used mainly as a means of informational security. Thus, in this document we will not discuss forensic biometric methods (such as DNA and AFIS) to which additional specific legal requirements apply, but rather methods to secure access to data or buildings.

The confusion mentioned above has led to uniformed comments as well as the growth of “urban myths” which can be addressed by Best Practices in a reasonable and appropriate fashion. Best Practices can then help to decrease confusion and establish real awareness of privacy impacts of biometrics and how to handle biometrics in practice in a privacy friendly and even enhancing manner. Therefore Best Practices can eventually mean help and guidance for all parts of an application: manufacturers, operators, system integrators and end-users. This draft is intended to redress the balance and reduce the confusion, offering practical advice to all involved in the use of biometric technologies. The aim is to create awareness among all parties dealing with biometrics.

We believe that this will contribute to the development of privacy-respecting and privacy-enhancing deployments. Privacy should be, next to technical, administrative and expenses aspects, one of the most important aspects to be addressed before and during the use of biometrics. For example, it should be considered when making the choice of which biometric is most suitable for the actual problem to be solved thus privacy compliance is a potential part of the practical guide of product selection.

Best Practices are seen as a supplementary to framework regulation. They are achieved by self- and co-regulation of industry, through interested associations, end-users and privacy and consumer advocates in an internationally approved manner. This document also suggests realizing the concept of Privacy Enhancing Technologies (PET) when using biometrics. PET must be understood as different measures in the area of communication- and information technologies that aim to protect privacy by means of elimination or reduction or protection of personal data without loss of functionality of the IT-system.

It is important to note that this document is not intended as Code of Conduct due to two main reasons. Firstly, it does not cover all aspects that should be considered
with biometric implementations and impacts on an individual using a biometric: aspects such as comprehensive education and information of the user. Secondly, it is primarily meant as a supplementary to framework regulation of the European Data Protection Directive according to a three level model:

1. Explanation of what the Directive requires when biometric data is used, thus what each biometric implementation must meet for being lawful (Must-Do),

2. Suggestions for interpretation of the legal framework for the practical use of biometric data (Interpretation and, to be added later on e.g. by national biometric working groups on the level of Member States, and

3. Proposals for a best way to handle biometric data also taking the concept of PET into account (Best Practice/PET).

Thus, it provides the legal framework to handle biometric data compliant with the European privacy regime, but suggests also a manner how to enhance privacy extending the requirements of the directive by means of PET.

It is important to note that this paper is not intended as a complete document ready to be used in practice. It is meant as a first draft to be further developed within the European Commission and each Member States and should be considered as contribution to tackle the discussion of privacy compliant and even enhancing biometrics.

II Objectives

This draft of Best Practices therefore aims to provide:


2. Guidance for System integrators: guidance for suppliers (i.e. manufacturers, middle ware developers, system architectures) in order to develop privacy compliant and even privacy enhancing biometrics from the beginning of a development of a biometric system.

3. Finally, information and assurance for end-users to learn about their rights when they are asked to use a biometric system/device and that these rights have been considered.

Basically, the aim is to make the biometrics community understand that privacy is not a hindering factor or an obstacle to it but rather an enabling factor to create a prosperous industry and successful products which do not intrude people’s privacy when implemented properly according to privacy principles which are not in theory but in practice realistic to handle (privacy as a competitive factor).
III Legal Framework for data protection in the European Union

The legal basis in Europe for treating personal data includes three main legal frameworks:

1 Treaty on the European Union, Title I - Common Provisions - Article F:
   - The Union shall respect the national identities of its Member States, whose systems of government are founded on the principles of democracy.
   - The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.
   - The Union shall provide itself with the means necessary to attain its objectives and carry through its policies.

2 European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8:
   - Everyone has the right to respect for his private and family life, his home and his correspondence.
   - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

3 European Union Data Protection Directive

This draft of Privacy Best Practices on Biometrics follows directly the European Data Protection Directive: “Directive 95/46/EC of the European Parliament and 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”\[1\]. It is intended to be a first step towards a common understanding of biometrics in the light of the privacy rights of the users of biometric systems. It will be given to the European Commission for discussion and further review and here especially to the Article 29 Working Party that has just begun to work on biometrics and is supposed to publish a first assessment and recommendation on biometrics after the end of the BIOVISION project in summer 2003.

\[1\] \url{http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm}
The point of view of the Directive has been chosen in order to be applicable to all European countries as a first assessment of how biometrics can be compliant to common European privacy principles and also be privacy enhancing. This draft is meant to be reviewed by all Member states after the end of the BIOVISION project to be specified in greater detail so as to meet the particular requirements of national legislation. This will be also an important task of the European Biometric Forum which is currently in the founding process by the BIOVISION team as one most relevant result of this project with respect to the future of the European community.

According to Art. 1 (1) of the Directive, the object of this directive is the following:

“In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” Recital (2) states: “Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals.”

The core values of the directive are also considered:

- reduction of the processing of personal data to the unavoidable extent,
- maintain the highest transparency possible,
- institutional and individual control of processing of personal data as efficient as possible, i.e. specific rights of the data subject with regard to his/her personal data.

The Directive can also be considered on the basis of 8 core principles with regard to processing of personal data which is regarded as fundamental in the following discussion:

- Fair and lawful processing (legal limitation or consent required);
- Specified, explicit and legitimate purpose (the finality principle);
- Respect for the right of the data subject;
- Data kept in a form which permits identification for no longer than necessary for the purposes for which the data were collected;
- Proportionality: adequate, relevant and not excessive;
- Accuracy and up-to-date;
- Appropriate technical & organisational measures against unauthorised use or unlawful processing;
- Data may only be transferred to those countries that ensure an adequate level of protection for the personal data.

---

2 Work on this is already being undertaken by members of the BIOVISION consortium in their countries, like TeleTrusT WG 6, Germany, and Biometrics Working Group, UK.
3 e.g. see chapter 2, No. 13: right to access, Art. 12 EC-Directive
Furthermore, specific categories of data are deemed to be especially sensitive and processing of this type of data is allowed only under specific circumstances, Art. 8. This will be also dealt with later in this document. Another condition that might be relevant to biometrics is Art. 15 which grants a right to individuals not to be subject to a decision that produces legal effects or significantly affects them, and is based solely on automated processing of data intended to evaluate certain personal aspects relating to them, for instance performance at work or creditworthiness.

It is important to note that Member States can extend protection to individuals beyond those mandated in the directive, in most cases. There can therefore be important differences in each Member State with regard to the assessment of biometric data in terms of privacy. A significant difference between Member States can also be established with regard to the obligation to notify the supervisory authority of specific data processing, Art. 18 and 19, and schemes of prior checking, Art. 20. For instance Art. 18 (1) states that Member States shall provide that the controller (…) must notify the supervisory authority (…) before carrying out any (…) automated processing operation (…). Yet according to Art. 18 (2)-(4) Member States may provide for simplifications or exemptions under certain defined conditions.

Art. 19 (1) states for instance that Member States shall specify the information to be given in the notification according to Art. 18, and only defines what the notification shall include as a minimum. Art. 20 states with regard to prior checking that “Member States shall determine the processing operations likely to present specific risks to their rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.”

Recital (53) adds in this context: “Whereas (…) certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they wish, to specify such risks in their legislation.” Whereas it is arguable whether or not and in which specific circumstances biometrics pose risks, different Member States might assess the risks differently. Since according to Art. 4 (1) (a) national law is applicable wherever the data processing is carried out on the territory of the Member State, the national law is decisive when discussing biometric data processing.

The Directive does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, Art. 3 (2), second hyphen. This means that for instance the use of a biometric system solely for the purpose of access to a private computer is not applicable for the Directive. Wherever the processing of biometric data occurs in the course of business, then the Directive will apply with all requirements therein.

4 National (federal & state) data protection legislation and privacy regimes
Last but not least national (federal) Laws & State Regulations are important for everybody who wants to use a biometric system in a specific application. These are not included in this document but are important for the national level of implementation and requirements of the national privacy regime. As for the Member States’ assessment of biometrics with regard to data protection the BIOVISION questionnaires on Biometrics & Privacy sent out to all 15 Data Protection Authorities will be supplementary and help to include the Member States’ interpretation of the Directive.

This draft is meant to be subject to review and further concrete application and interpretation by the European Member States. Its intention is to trigger the discussion of privacy compliant and even enhancing biometrics along with the increasing number of implementations in Europe.

IV European Framework for Best Practices

The European Data Protection Directive states in recital (61) that “member states and the Commission, (…), must encourage the trade associations and other representative organisations concerned to draw up codes of conduct” so far as to facilitate the application of the directive. Furthermore, recital (26) states that “codes of conduct in the meaning of article 27 may be a useful instrument in providing guidance as to the way in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible”.

Article 27 states in § 1: Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions (…), taking account of the specific features of the various sectors. And in § 3 it says: Draft Community codes (…) may be submitted to the Working Party referred to in Article 29.

The European Initiative on Privacy Standardisation in Europe suggests in its final report the creation and establishment of voluntary Best Practices made available free or at low cost to help business and data managers ensure that they are compliant with the Directive and, where possible and appropriate, the diverse European national laws and additional requirements (recommendation 1). This work is supposed to be realised as soon as possible. It is also proposed that this activity takes place in the open consensus environment provided by the European standardisation, e.g. in a CEN/ISS-workshop or an equivalent forum. The BIOVISION Roadmap programme is the appropriate forum to set up a draft and discuss this within those long established and approved as CEN. It is also meant to

---

4 The final report of the BIOVISION project team which will be publicly available will include the questionnaire and a summary of all replies received.
5 Already work on the national level has begun on basis of this document in Germany in the TeleTrusT Working Group 6 Biometrics and in the UK in the CESG Biometric Working Group.
6 European Data Protection 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 as of 24.10.1995
complement and support the work of the Article 29 Working Party that has recently started to work on a first assessment of biometrics in December 2002.

V Understanding biometric data with regard to privacy

1 The meaning of privacy in terms of biometrics

With increasing numbers of biometric implementations worldwide, the aspect of privacy gains importance. As a result, before having a close look at the details it is necessary to understand what the objectives of data protection law and policy intends. Stated simply, it is the protection of the personal rights of those, whose data are processed, and the protection of individuals and not simply the protection of data that we are concerned with.

Depending on how a system is deployed biometrics can either threaten or protect an individuals privacy. The possibility of protection is especially valid in view of the special properties of biometrics, which for an entire life are linked to the individual unlike Pins and Passwords which are only indirectly and weakly linked to a person. Therefore, by using biometrics, other types of personal data can be better protected from theft and misuse than by traditional means. As a result we have to understand both the threat and protection potential of biometrics when discussing it in terms of privacy: on one hand, biometrics as potential personal data which needs to be protected in the same way as any other personal data, on the other hand biometrics as a new and better means to protect other personal data in the context of data security. Biometrics can therefore be both an object and tool in the different aspects of this discussion.

In a positive way biometrics can be seen as privacy protector, because:

- Biometric authentication can provide a better personal binding of access rights to personal data than traditional means like PINs and passwords, e.g. better access control to areas where personal data is held;
- Protection of Identity Theft: ensuring personal data can be linked exclusively to the right person and therefore can only be used in the name of the right person.

In a negative way, biometrics can present a potential threat to privacy because:

- If biometrics become compromised: there can be no reconstruction or revocation if the original characteristic is “burned.”
- If biometrics were seen as a very strong means of authentication, proof of misuses by impostors would be impossible or at least very difficult & expensive.

7 Whereas establishing public-key-infrastructures or other measures of protecting biometric images and templates as part of a system might help in this regard.
2 Some fundamental principles to be considered when using personal biometric data

There are some common principles that must be considered when implementing biometrics in real world applications according to European law. It is important to note that in some Member States’ their individual legal particularities will lead to different interpretations. However, some of the commonly understood aspects are listed below:

• **Proportionality principle:**
  
  o Rights of the data subject & interests of the data controller must be balanced (meriting interests of the data subject):

  Possible additional (“superfluous”) information, e.g. DNA (medical and ethical information) need to be taken into account, referring also to Art. 8 of the directive (see below for further explanation);

• **Potential Risk of Discrimination:**

  o Inability for an individual to be enrolled to a biometric system can cause discrimination as the use of biometrics becomes more prevalent in large scale everyday environments;

  o False Rejection can have serious consequences especially in governmental applications, e.g. border control; also creates false suspicion in terms of criminal justice needs to be considered;

  o False Acceptance can lead to incorrect data for enrolled individuals;

  o If biometrics become regarded as a very strong and tamper-proof authentication (perceived reliability): maintaining the presumption of innocence and the expenses to disprove the contrary can be a problem for the individual (questioning biometrics can become extremely difficult in the everyday and the legal realm);

  The true reliability will be crucial: the risk of false positives and false negatives must be considered; if e.g. a criminal conviction is being sought and the decision hinges on information produced from a biometric system, the court must be sure that the false rates of the system are known and are accurate in practice, not only in theory;

• **Improper Use/Finality Principle/Scope Limitation/’Function Creep’:**

  o Mostly lifelong binding of biometric data to the data subject:

---

8 BIOVISION Workpackage 5 on medical impacts of biometrics is considering also this aspect and must be seen as addition to this document.

9 If the high reliability of the used biometric can be proved then in a related way any potential biometric might also increase its forensic value for criminal actions.
Automatic processing of biometric data can lead to widespread use for a purpose other than the purpose for which that data was collected originally; a biometric represents in general the potential basis for a ubiquitous identification scheme and therefore creates the possibility to track movements and behaviour, detailed profiles by compilation of transactional information about a particular person that creates a picture of travels, preferences, affiliations or beliefs; this can also create a temptation to make use of powerful databases not only by totalitarian governments but also by democratic regimes which can occur when they feel the end justifies the means; this applies not only to governments but also and in particular to the private sector which is likely to have large biometric databases in the future: potential risk of uncontrolled matching or linkage to different databases;

- The possible reduction in transparency and loss of control can undermine the informational privacy.

- **Possible covert obtaining of biometric data and monitoring:**
  - Some systems are more likely to obtain biometric data without consent or even knowledge of the data subject than others, depending on the activity required from the user to undertake the collection process;
  - Obligation to announce any surveillance in public places is required depending on national law;
  - General prohibition of covert monitoring e.g. at workplaces, can also be relevant again depending on national law;

- **Specific data warranting protection:**
  - Special categories of data as sensitive data can be applicable to biometrics, see Art. 8 EC-Directive and below;
  - Meriting interests of the data subject must be taken into account, in detail mainly according to national law

- **Automated decision taking**, see Art. 15 EC-Directive and below;

- **Biometric as “identification number” (“unique identifier”):**
  - See Art. 8 (7) Directive: “Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.”, thus depending on national law.

This list is not complete and is just intended to show possible impacts of biometrics in terms of fundamentals of data protection rules.
VI Privacy Enhancing Technologies (PET) in the context of biometric data

The principle of PET applies to biometrics from two standpoints: firstly, the implementation and application of biometrics has to follow a correct privacy regime in order to be privacy enhancing. Secondly, biometrics itself can be a privacy enhancing method. For instance, the European Initiative on Privacy Standardization in Europe speaks in its final report of biometrics as a tool of Privacy Enhancing Technologies\[10\]. The main question according to the concept of PET is whether or not “identity” is necessary for each of the processes of the conventional information system? In most cases it is not necessary to know the user’s identity in order to grant privileges. Yet there are some situations in which the user must reveal his or her identity to allow verification. In these cases, some general rules can be suggested, i.e. for instance:

- Use as little personal data as is necessary for the aim of authentication,
- If using personal data, use means of encryption,
- Destroy raw data as soon as possible,
- Anonymize personal data whenever possible,
- Do not use central databases where not required\[11\],
- Give users control over their personal data (“identity protector”),
- Use means of evaluation and certification to create a guaranteed level of trust.

VII The biometric system process

In order to understand the privacy implications of biometrics the principle of a biometric system process needs to be understood. The generic biometric system processes can be broken down into five major groupings:

- Data Collection
- Transmission
- Signal or Image Processing
- Matching Decision
- Storage

1 Data Collection

A biometric sample is collected using a sensor, which could be of many types, e.g. an optical, or silicon based fingerprint sensor or a camera. The sensor captures an image of the biometric, or some form of input e.g. from a keyboard in the case of keystroke dynamics or the dynamic properties of a handwritten signature. The data collected is biometric raw data.

2 Transmission

\[10\] CEN/ISSS Final report, 4.26
\[11\] Prohibited for instance in Germany according to the use of biometrics in ID-cards and passports.
The biometric image is usually then transmitted (all be it internally within the sensor) and may be compressed in order to reduce the file size and therefore the required bandwidth and subsequent transmission time. If the image has been compressed it is usually then uncompressed before feature extraction is applied. Implementation of some form of encryption or signing of raw data might be found either embedded to a biometric product, or engineered into the integrated system architecture.

3 Signal or Image Processing

The image is subjected to feature extraction techniques using a proprietary algorithm. These algorithms take the raw image or input data and extract whatever relevant features are required to turn this into a mathematical format which is the core of the biometric systems functions. The features that are extracted will vary between biometric technologies. It may be that individual ‘minutiae’ points from a fingerprint are located and their relative positions used to create the template, or that the characteristics of a hand such as finger length, width of palm etc are used as in hand geometry systems. The extracted features are usually referred to as the ‘biometric template’.

In most biometric technologies a quality control algorithm is applied, either after the feature extraction has taken place, or in some cases using firmware embedded in the sensor. This may be based on a number of factors, such as the number of fingerprint minutiae extracted from a fingerprint image. Should the quality measure be too low there may be a request for more raw data to be captured.

If the template is of sufficient quality it may be stored either in a database, or in a token such as a smart card, or it may be passed directly to a matching process whereby the new template is compared against either a single stored template (one to one comparison), or searched against a number of earlier templates stored in a database (one to many comparisons).

4 Storage

In the majority of biometric systems in use for non-governmental systems, unrelated to law enforcement systems, then any storage tends to be of the template only. After the image has been processed and an adequate quality template produced, most biometric systems discard the original image. However, it is possible (particularly in law enforcement or facial recognition systems) that the original image is retained, as human decision making processes may have to be applied or interoperability with other algorithms applied at a later stage is to be ensured.

In many one-to-one type systems templates are located in a database by means of a unique reference, such as a PIN number, or using a token form of identifier, alternatively the template may be located only on an identifying token and on no other database.

5 Matching Decision
All biometric systems have a matching decision stage where templates are compared in order to ascertain how closely these match. The result of this process is reported in a number of ways depending on the particular system, or operator requirement. For verification, that is one-to-one systems, the decision required is usually for a simple ‘yes/no’ i.e. the presented template is, or is not a close enough match. The acceptable level of confidence that the two templates come from the same person depends on the setting by the system operator of a decision ‘threshold’ related to this process.
1 In what cases are biometric data personal data?

EC-Directive Art. 2 (a) defines personal data as any information relating to an identified or identifiable natural person. This person is described as “data subject” which is “an identifiable person 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”.

The Directive is intended to be applicable in particular to processes involving data derived from “the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons” in the information technology society, see recital (14). And recital (26) states in more detail what is meant by “an identified or identifiable person: “Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible”.

The Directive defines personal data in a very global sense in order to cover all information that can be related to a natural person. Thus, the Directive is open to cover also biometric data such as photographs and voice, fingerprints and also genetic features. In single applications, depending heavily on what data is stored exactly (see explanation of the biometric system process above), the biometric data in case might not meet this broad definition of personal data. Biometric data can occur as raw data and templates in general. Whereas raw data is in most cases the original image of the chosen characteristic, e.g. fingerprint, face or iris, the template contains only a hash code of the original data which is derived from the original and calculated in a mathematical manner. From the biometric template the state of the art is that the original can barely be reconstructed.

However this depends also on the architecture of the system and here within e.g. on the amount of information which are processed for creating the template. If the reconstruction is not possible, a template can be seen as pseudonymous data which does not mean that this data is no longer personal data but does make it more difficult technically to identify the person behind the data. If the template is stored in a manner that a link to the person is no longer possible and excluded,

---

12 See for further details and possibilities of reconstruction Bromba, On the reconstruction of biometric raw data from template data, http://manfred.bromba.bei.t-online.de/biometrics/temppriv.htm
then the template ceases to be personal data. However in most cases a link to the person who is supposed to be identified is possible at least for the data controller, to check finally the proper functionality of the system and cases of false rejects or false matches. Therefore, in most cases the obtained, processed and stored data are most likely to be regarded as personal data within the meaning of the Directive.

Possible personal data that relate to the implementation of a biometric can include:

- the image or record captured from the sensor at the initial enrolment
- any transmitted form of the image or record between sensor and processing systems;
- the processed data, whether completely transformed to a template or only partially processed by an algorithm;
- the stored image or record or template;
- any accompanying data collected at the time of enrolment;
- the image or record captured from the sensor during normal operation of the biometric (verification of identity or identification);
- any transmitted form of the image or record at verification or identification;
- the template obtained from the storage device;
- any accompanying data obtained at the time of verification or identification;
- the result of the matching process when linked to particular actions or transmissions;
- any updating of the template in response to the identification or verification.

With regard to this, although it might not be true for all applications in all cases, in the meaning of Best Practices we recommend to treat biometric data always as personal data. We recommend also storing only such biometric data that are necessary for the need of the authentication process. In the case of PET this can also mean to use verification wherever identification is not needed for the purpose of the application. If storage apart from the identity means itself is necessary for the needs of the application no biometric data with superfluous and additional information should be stored.

2 What does processing of data mean?

EC-Directive Art. 2 (b) defines processing as any operation or set of operations which is performed upon personal data, (…), such as collection, recording, organisation, storage, adoption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Above the general process of data in a biometric system was described. In the meaning of the Directive, all processes in a biometric system are considered as processing of data.

3 Who can be the data controller or the processor?

17
According to EC-Directive Art. 2 (d) the controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

EC-Directive Art. 2 (e) defines processor as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

In this meaning the data controller or processor of biometric data will be in most cases the operator who runs the system. Thus it is up to him or her to meet many of the privacy requirements discussed in this document.

4 What has to be considered with regard to the data subject?

According to EC-Directive Art. 7 (a) personal data may only be processed if the data subject has given his consent unambiguously. Art. 7 is the central rule for the lawfulness of processing personal data and contains a complete catalogue of cases in which the Member States can allow the processing of personal data. One of the conditions is the consent of the data subject. This means that provision of consent prior to the processing can make the processing of personal data lawful. This is important in particular in such cases where the processing is not lawful according to the other legitimate purposes stated in Art. 7 (b) – (f).

According to recital (30) in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding.

Yet it must be noted that asking for the data subject’s consent only makes sense in applications in which the user is genuinely free to refuse consent without significant detriment, thus if the refusal will mean no processing of biometric data. There may be circumstances such as employment where genuine consent is difficult to achieve. In these cases, another legitimate purpose may need to be relied on.

5 What is meant by consent?

EC-Directive Art. 2 (h) defines the data subject’s consent as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
Only such a consent which meets these requirements can make the processing lawful. In other words, a consent that does not match with these requirements is worthless and the processing remains unlawful apart from those cases Art. 7 (b) – (f) applies in the meaning mentioned above.

There may be circumstances where it is not practicable or not possible to obtain freely given consent, e.g. where provision of a biometric is a condition of employment. In these cases for the processing to be lawful one of the other provisions of Art. 7 (except in cases of Art. 7 (b)-(f) must be applicable.

The consent applies to a concrete processing of the personal data of the data subject by a definite controller for a clear purpose. In order to meet these requirements the controller has to inform the data subject of

a. the controller himself (acc. to Art. 2 (d) the controller is the natural or legal person (…) which (…) determines the purpose and means of the processing of personal data),

b. the actual processing of data and,

c. of the purpose of the data processing.

**6 What does freely given specific and informed indication mean?**

Before giving his consent the data subject has to be informed of the manner in which his biometric data are processed (acc. to the definition in Art 2 (b) mentioned above) in order to be able to give his informed consent. It is not sufficient just to tell that personal data are processed abstractly but the concrete situation and application has to be explained. The best way to do this is not only to explain to people the situation but to provide them e.g. with leaflets in which the data processing is explained in detail.

A freely given indication requires a free and self determined decision without any compulsion. An informed consent requires comprehensive information from the controller. The information to be given to the data subject is specified in Art. 10 and 11.

Art. 10 for instance applies to cases of collection of data from the data subject and requires:

(a) the identity of the controller and of his representative, if any,
(b) the purposes of the processing for which the data are intended,
(c) any further information such as:

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him in so far as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.
Furthermore, consent can be withdrawn by the data subject without reason so the data controller must be able to cope with this. This means e.g. deleting biometric data from a database or discarding any token on which the biometric data was stored without any remaining data that could be linked to the individual.

7 Are there any formal requirements for the expression of consent to be legally valid?

The consent does not have to be in written form or even explicit, an implied consent is sufficient. Also an oral and an electronic consent is enough to fulfil the legal requirement. Details also depend on national law.

8 Can the processing of biometric data be lawful when sensitive data is used?

Yes, EC-Directive Art. 8 (1) defines sensitive data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

8a What requirements must be fulfilled when processing sensitive data?

According to EC-Directive Art. 8 (2) there is a general prohibition of processing sensitive to which some exemptions apply. An important exemption is met when the data subject has given his/her explicit consent to the processing of those data (apart from some exemptions mentioned in Art. 8 (2) (a) - (e)). This means processing sensitive biometric requires the explicit consent of the data subject.

8b In which cases can biometrics be sensitive data?

Additional information can be revealed by any biometric in general, but this heavily depends on the specific biometric characteristic used for the authentication purpose (e.g. when using faces in automated facial recognition systems ethnic and racial origin is more likely to revealed than with iris-scan or hand-geometry) and the application itself. Also the possibility of such revealing information is depending upon whether raw data or templates are processed. The theoretical possibility of deriving such data from a biometric ought not be a problem in practice provided the data controller makes no attempt to actually make use of such sensitive data.

- Sensitive data in terms of biometrics can include medical (e.g. iridology, even if this is not academically proven to date), ethnic/racial, specific sort of behavioural information like trade-union membership or data concerning sex life.
In the meaning of Best Practice, we recommend implementing a biometric system in a manner where superfluous data cannot be used at all. In the meaning of PET, already obtaining and collecting such data should be technically impossible.

**8c. What does explicit consent mean in comparison to the usual content?**

In this case, an implied consent is not enough. The expression of consent must specify the particular sort of (sensitive) data that are to be processed. This can apply, e.g., to facial recognition where false matches can be based on medical or ethnic reasons, and therefore the controller needs to be able to find out why the system does not work properly and thus possibly reveal those information. The case of explicit consent to this data could not therefore infer from a general consent given to this use of facial recognition.

**9. What further information should be given to the user of a biometric system with regard to privacy?**

In the meaning of Best Practices, in addition to that information, you have to provide for the consent it would be desirable to inform the user of your specific information handling and privacy protection practices.

This can include the security safeguards principles that are in place within your biometrics application, e.g.:

- Security level for biometric system itself,
- Limited access and access control,
- Biometric data stored separately from any other identifying information.

**10. What rights does the data subject have to the processing of their biometric data?**

EC-Directive Art. 14 states the data subject’s right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. Recital (30) states the processing of personal data, in order to be lawful, must be carried out with the consent of the data subject or be necessary for one or several reasons (e.g. with a view to the conclusion or performance of a contract binding on the data subject or be required e.g. of a task in the public interest). In each case, it must be provided that the interests or the rights and freedoms of the data subject are not overriding. This applies at least for the cases referred to in Art. 7 (e) and (f) which concern the case when processing personal data 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 (e), and when processing is necessary for the
purpose of the legitimate interests pursued by the controller (...) except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Member states are free to widen this right also for other cases according to recital (30) and (45). This requirement is also an example for the application of the proportionality principle (see above in the introduction).

As part of our work on Best Practices we recommend the use of participative or co-operative biometric systems where possible so that biometric data is collected with consent and knowledge

11 What does reasonable access to the personal data of the data subject mean?

EC-Directive Art. 12 states that every data subject has the right to obtain from the controller specific information, e.g. the categories of data concerned etc about them. Recital (41) states that the data subject must be able to exercise the right of access to data relating him which is being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing. This includes:

- confirmation as to whether or not data relating to him is 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 is 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 Art. 15 (1) that refers to automated individual decisions.

In practice this might be difficult to handle for the data controller who actually has to reveal any information about which kind of system is used in the given application, e.g. whether raw images or templates are processed and in which actual technical and logical manner. Implemented biometric systems are usually very complex and able to carry out much more processing than that which may affect the actual data subject who requires the information. In general the data controller only has to reveal the processing actually concerning the individual itself and not the overall operating system entirely. A practical approach might be to offer a re-registration, followed by a comparison between stored and new template.

12 What has the data controller to do to ensure that the processing of the biometric data is done fairly and lawfully?
EC-Directive Art. 6 (1) states that personal data must be processed fairly and lawfully.

According to recital (28) this means in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed, and such purposes must be explicit and legitimate and must be determined at the time of collection of the data. The purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified. Thus, this requirement is a detailed definition of the principle of proportionality and the finality principle.

13 What does security of processing mean?

The data controller must ensure that unlawful processing of biometric data does not occur or is very unlikely. According to EC-Directive Art. 17 the security of processing has to be ensured by means of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

Recital (46) states in this context that the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing.” It is also incumbent on the Member States to ensure that controllers comply with these measures that must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

The realisation of the security of processed biometric data is subject to national legislation and therefore up to interpretation of the Member States. They can provide special data security models which are to be met or specific requirements also for biometric data in particular. The Directive only requires an appropriate level of security. Ways of protecting biometric data can include access limitation, and ensuring that the original data cannot be derived from the template, thus the encoding must be appropriately secure.

Within the meaning of Best Practices and the concept of Privacy Enhancing, we recommend encoding biometric data as soon as possible. Use only templates but not raw data whenever possible and destroy raw data as soon as possible (see also introduction below on PET). If however images are required for the operation of the system then they must be appropriately protected. Do not use identification when verification suffices for the application in place. We also recommend to rather use decentralised storage than central databases whenever suitable for the given application. This is because their appropriate protection in a central database always requires, under others, the thorough control of strict access rights and, when encrypting is in place, also proper key management. This is in practice often difficult to realise, thus a latent risk of misuse exist and function creep (see below)
can more easily occur than with storage under the control of the data subject. Moreover, providing the user with the control over his/her biometric data can provide higher transparency. This does not mean to absolutely avoid central databases, and of course they are not generally prohibited under privacy laws, but within a sensible handling of biometric data the secure storage of biometric data should always be considered as crucial aspect. Furthermore we suggest to set up a level of guaranteed trustworthiness e.g. by means of evaluation and certification. This can mean to use Technical Recommendations as Best Practices of the Biometric Working Group in the UK13.

14 How can biometric data be kept up to date and accurate?

EC-Directive Art. 6 (d) states that data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is erased or rectified.

In terms of biometrics this means to use only such biometric systems that have low false match rates so there is little likelihood of leading to incorrect data of the entitled individual. The data controller has also to provide means of detection and identification of false matches (protocol etc.) in order to establish means to correct incorrect biometric data. With regard to the privacy rights of the data subjects, a single system might be rejected due to privacy breaches even though it has very low false matches if this is not acceptable for the specific application regarding the rights of the concerned individuals.

15 What does the obligation of notification imply (compliance regime)?

EC-Directive Art. 18 (1) states an obligation to notify the 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. Art. 19 defines the necessary contents of the notification that shall include at least:

- the name and address of the controller and of his representative, if any,
- the purpose or purposes of the category or categories of data subject and of the data or categories of data relating to them,
- the recipients or categories of recipient to whom the data might be disclosed,
- proposed transfers of data to third countries,
- a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Art. 17 (that concerns the security of processing).

The EC-Directive intends that when processing data is done according to the general principle of transparency. Art. 18 (2) allows Member States to provide for the simplification of or exemption from notification in specific circumstances.

This can be the case e.g. where the data controller appoints a data protection official to ensure that the rights and freedoms of the data subject are unlikely to be adversely affected by the processing operations. In any case the data protection official must consult the authority in cases of doubt.

16 In what cases does biometric data processing require prior checking by the supervisory authority?

EC-Directive Art. 20 states that Member States shall determine processing operations likely to present specific risks for the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

It is not easy to determine when a biometric system does present "specific risks" in that sense. The assessment of possible risks by biometrics is mainly subject to interpretation of the Member States and can lead to (non) authorisation of biometric data processing, although several exemptions are provided according to the directive which can lead also to exemptions in national law. See also the introduction on this aspect.

17 Does the restriction for automated decision taking apply for biometrics?

According to EC-Directive Art. 15 (1) „Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”

This might be applicable to those decisions bound solely to a biometric system and not additionally checked by an individual provided that the system actually evaluates certain personal aspects what most biometric systems do not. For instance denying someone a passport or entry into an aircraft might be subject to this requirement. This would mean that a human intervention would have to be involved before a final decision is taken. In practice this might well be the intention of the system operator.

Examples of an automated decision using biometrics means might, according to the directive, include border crossing and immigration processes in the public sector or biometric systems at the working place in the private sector.

Note that Art. 15 provides important exemptions:

2 (a): if the decision is taken in the course of entering into or performance of a contract, provided the request by the data subject has been satisfied, or that
there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to defend his point of view; or

2 (b): if the decision is authorised by a law which also lays down measures to safeguard the data subject’s legitimate interests.

In cases when the biometric system is only used to support an authentication process and the legal decision is not based solely on the biometric process, Art. 15 ought not apply for the biometric data processing.
Overview of the EU data protection environment for biometrics

A significant amount of effort was devoted to obtaining an overview of the situation in the individual member states with regard to biometrics and the data protection requirements. The questionnaire below was prepared and provided to each of the national data protection offices. As a result we were able to start compiling an understanding of the position in each of the Member States.

The BIOVISION Project Group questionnaire to European Data Protection Commissioners

1. Did your country already transpose the EU-Data Protection Directive 95/46/EC? If yes, how did you do it?

2. Is there any existing specific legislation in your country regulating obtaining, using, processing and transferring biometric data?

3. If your answer to question 2 was YES, do they distinguish between governmental and private use?

4. In terms of storage of biometric data, which one do you prefer when biometric data are used: centralised storage or storage under control of the user, e.g. on a card or another token?

5. Do you consider biometric data as personal data or even sensitive data in the sense of Article 6 EU-Data Protection Directive 95/46/EG? If yes, are there specific conditions on the processing of those data according to your country’s regulations?

6. Does it make a difference whether biometric raw data or templates are stored, used, processed or transferred?

7. Are there any licenses, limitations or Best Practices in use in terms of manufacturing and operating biometrics? If yes, please describe which ones and for which applications/operators.

8. Are you aware of any current usage of biometrics in your country? If yes, please describe in which applications (gov./private) and with which goal (positive or negative identification/verification). Do you have any objections against a special kind of use? Why/why not?

9. Do you have a preference for certain biometrics in terms of data protection? If yes, which one, and why?
10. Do you suggest any procedures in using biometrics not only in a privacy friendly but enhancing way, for instance preferably or exclusively anonymous or encrypted?

11. What do you think of the “Privacy Enhancing Technologies” - concept in terms of biometrics?

12. Is the use of biometrics approved with regard to electronic signatures? Are there any specific regulations in terms of biometrics within electronic signatures?

13. Have you made any statements on biometrics that are available and you can add to your replies?

14. Please give a reason for your answer in each question as comprehensive as possible.

15. Please provide a web-address where mentioned regulations and politics could possibly be found, or add a hardcopy if available in English, or French/Italian/Dutch.
<table>
<thead>
<tr>
<th>Questions</th>
<th>Germany</th>
<th>Portugal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there existing legislation regulating obtaining, using, processing and transferring biometric data?</td>
<td>Yes, in the counterterrorism-legislation (Terrorismusbekämpfungsgesetz as of 9. January 2002, article 8). Biometrics can be implemented in ID cards and passports</td>
<td>No</td>
</tr>
<tr>
<td>Do you distinguish between governmental and private use?</td>
<td>Yes, only for governmental use (identification card and passport).</td>
<td>n/a</td>
</tr>
<tr>
<td>Re biometric storage- do you favour centralised storage or on a card or another token?</td>
<td>Under data protection aspects we prefer the storage under control of the user.</td>
<td>n/a</td>
</tr>
<tr>
<td>Do you consider biometric data as personal data or even sensitive data in the sense of Article 6 EU-Data Protection Directive 95/46/EG? If yes, are there specific conditions on the processing of those data according to your country’s regulations?</td>
<td>Biometric data are personal data or even sensitive data in the sense of the Directive Article 6 EU. Regulated in the German Data Protection Act.</td>
<td>Our Commission considers biometric data as personal data, in the sense of the Directive and of our Law 67/98. The Commission is currently discussing if all or some of those data are sensitive data.</td>
</tr>
<tr>
<td>DOES IT MAKE A DIFFERENCE WHETHER BIOMETRIC RAWDATA OR TEMPLATES ARE STORED, USED, PROCESSED OR TRANSFERRED?</td>
<td>There is a difference between rawdata and templates. Rawdata can be very sensitive, templates can be sensitive data. Both are private data and have to be handled in that way (encrypted)</td>
<td>n/a</td>
</tr>
<tr>
<td>ARE THERE ANY LICENSES, LIMITATIONS OR BEST PRACTICES IN USE IN TERMS OF MANUFACTURING AND OPERATING BIOMETRICS? IF YES, PLEASE DESCRIBE WHICH ONES AND FOR WHICH APPLICATIONS/ OPERATORS.</td>
<td>Yes. As long as biometric data are personal data is their use regulated in the data protection act.</td>
<td>n/a</td>
</tr>
<tr>
<td>Are you aware of any current usage of biometrics in your country? If yes, please describe in which applications (gov/private)</td>
<td>Used for personal identification/verification systems for a variety of different applications in the private sector. For governmental use there are</td>
<td>The use of biometric data is recently increasing in Portugal. They are mostly used to control the abiding of workers and civil servants. For this purpose Fingerprints are mainly used (and</td>
</tr>
<tr>
<td>applications (gov./private) and with which goal (positive or negative identification/verification). Do you have any objections against a special kind of use? Why/why not?</td>
<td>applications not announced; but gov. organisations are testing different systems for their usability for special tasks.</td>
<td>Fingerprints are mainly used (and, in a lesser degree, the iris recognition system).</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>DO YOU HAVE A PREFERENCE FOR CERTAIN BIOMETRICS IN TERMS OF DATA PROTECTION? IF YES, WHICH ONE, AND WHY?</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>DO YOU SUGGEST ANY PROCEDURES IN USING BIOMETRICS NOT ONLY IN A PRIVACY FRIENDLY BUT ENHANCING WAY, FOR INSTANCE PREFERABLY OR EXCLUSIVELY ANONYMOUS OR ENCRYPTED?</td>
<td>As long as there is a reference to persons all biometrics data have to be encrypted (data protection aspects). In the process of the enrolment only the templates should be stored and processed.</td>
<td>n/a</td>
</tr>
<tr>
<td>WHAT DO YOU THINK OF THE “PRIVACY ENHANCING TECHNOLOGIES”-CONCEPT IN TERMS OF BIOMETRICS?</td>
<td>The data protection supports “Privacy Enhancing Technologies”. Biometrics can improve PET within the realms of possibility of the application.</td>
<td>n/a</td>
</tr>
<tr>
<td>Is the use of biometrics approved with regard to electronic signatures? Are there any specific regulations in terms of biometrics within electronic signatures?</td>
<td>unknown</td>
<td>n/a</td>
</tr>
<tr>
<td>Have you made any statements on biometrics that are available and you can add to your replies?</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Questions</td>
<td>Denmark</td>
<td>Sweden</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HAVE YOU TRANSPOSED THE EU-DATA PROTECTION DIRECTIVE? HOW?</td>
<td>Directive 95/46/EC was transposed into Danish law by legislative Act no. 429 of 31 May 2000. An English version of the Act can be found at the following html: <a href="http://www.datatilsynet.dk/eng/index.html">http://www.datatilsynet.dk/eng/index.html</a></td>
<td>The EC Data Protection Directive 95/46/EC has been implemented through the Personal Data Act (adopted by the Swedish Parliament) and the more detailed Personal Data Ordinance (adopted by the Swedish Government). This legislation came into force on 25 October 1998 and replaced the Data Act which had been in force since 1973.</td>
</tr>
<tr>
<td>Is there existing legislation regulating obtaining, using, processing and transferring biometric data?</td>
<td>No specific legislation exists regarding biometrics however, the processing of biometric data is covered by the Danish Act on Processing of Personal Data.</td>
<td>No, not regarding biometric data as such. See below under 8.</td>
</tr>
<tr>
<td>Do you distinguish between governmental and private use?</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Re biometric storage- do you favour centralised storage or on a card or another token?</td>
<td>In previous decisions the DPA has held that the storage of biometric data on a card held by the data subject himself was permissible. However, it may very well be possible that a situation where the data is stored in a central database could also be found to be in accordance with the Act on Data Processing.</td>
<td>If data are stored on the user`s card etc., it is of course easier for him/her to control in which situations his biometric data are collected.</td>
</tr>
<tr>
<td>Do you consider biometric data as personal data or even sensitive data in the sense of Article 6 EU-Data Protection Directive 95/46/EG? If yes, are there specific conditions on the processing of those data according to your country’s regulations?</td>
<td>Biometric data is considered personal data in the sense of Article 6 in Directive 95/46/EC. However, whether the data is classified as sensitive or as non-sensitive depends upon whether the biometric can reveal sensitive information such as ethnic background or information about the data subjects health. Both in regards to situations where the biometric is regarded as non-sensitive, and as sensitive will the processing have to take place under the observance of the normal rules in the Act on Data Processing.</td>
<td>Biometric data that provides such information as is listed in article 8.1 of the Directive is to be considered as sensitive data. Processing of such data is only permitted in those situations listed in sections 14-19 of the Personal Data Act.</td>
</tr>
<tr>
<td>DOES IT MAKE A DIFFERENCE WHETHER BIOMETRIC RAWDATA OR TEMPLATES ARE STORED, USED, PROCESSED OR TRANSFERRED?</td>
<td>The fact whether the biometric can be recreated and used to compromise the integrity of the data subject, may in a given case be considered a vital element.</td>
<td>n/a</td>
</tr>
<tr>
<td>ARE THERE ANY LICENSES, LIMITATIONS OR BEST PRACTICES IN</td>
<td>There is a Danish decision (attached below) of the DPA’s decision regarding BornholmsTrafikken, which dealt with biometric as an means of identification. In addition berate an HO-convention.</td>
<td>n/a</td>
</tr>
<tr>
<td>Question</td>
<td>Response</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USE IN TERMS OF MANUFACTURING AND OPERATING BIOMETRICS? IF YES, PLEASE DESCRIBE WHICH ONES AND FOR WHICH APPLICATIONS/ OPERATORS.</td>
<td>addition hereto, an ILO convention concerning Seafarers Identity Documents is currently being negotiated. It is expected that these SID’s will include biometric information regarding the individual seafarer. For further information please consult the ILO webpage: <a href="http://www.ilo.org">www.ilo.org</a>.</td>
<td></td>
</tr>
<tr>
<td>Are you aware of any current usage of biometrics in your country? If yes, please describe in which applications (gov./private) and with which goal (positive or negative identification/verification). Do you have any objections against a special kind of use? Why/why not?</td>
<td>No, however, it is preferred, as mentioned under 5, that the biometric does not reveal sensitive information regarding the data subject.</td>
<td>The Police Data Act (1998:622) contains specific provisions regarding the Police’s processing of fingerprints etc. for the purpose of identifying persons in connection with a committed crime and also for identifying unknown persons in other situations. The police may only process data about fingerprints regarding persons who are suspected of having committed a crime, have been sentenced for committing a crime or persons whose fingerprints have been taken in accordance with the Act (1991:572) concerning special controls in respect of aliens.</td>
</tr>
<tr>
<td>DO YOU HAVE A PREFERENCE FOR CERTAIN BIOMETRICS IN TERMS OF DATA PROTECTION? IF YES, WHICH ONE, AND WHY?</td>
<td>no</td>
<td>n/a</td>
</tr>
<tr>
<td>DO YOU SUGGEST ANY PROCEDURES IN USING BIOMETRICS NOT ONLY IN A PRIVACY FRIENDLY BUT ENHANCING WAY, FOR INSTANCE PREFERABLY OR EXCLUSIVELY ANONYMOUS OR ENCRYPTED?</td>
<td>Currently PET technologies are still at an early stage, and have therefore not been dealt with by the DPA in concrete cases.</td>
<td>n/a</td>
</tr>
<tr>
<td>WHAT DO YOU THINK OF THE “PRIVACY ENHANCING TECHNOLOGIES”-CONCEPT IN TERMS OF BIOMETRICS?</td>
<td>no</td>
<td>n/a</td>
</tr>
<tr>
<td>Is the use of biometrics approved with regard to electronic signatures? Are there any specific regulations in terms of</td>
<td>As mentioned under 8, see the DPA’s decision regarding BornholmsTrafikken.</td>
<td></td>
</tr>
<tr>
<td>biometrics within electronic signatures?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Have you made any statements on biometrics that are available and you can add to your replies?</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Questions</td>
<td>UK</td>
<td>France</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HAVE YOU TRANPOSED THE EU-DATA PROTECTION DIRECTIVE? HOW?</td>
<td>Yes, transposed as the Data Protection Act 1998</td>
<td>Not yet. But believe the directive is 95% translated. The legislative process is still on going (lecture 2nd quarter 2003 in higher chamber).</td>
</tr>
<tr>
<td>Is there existing legislation regulating obtaining, using, processing and transferring biometric data?</td>
<td>No only general data protection legislation</td>
<td>No and biometrics is not defined by law</td>
</tr>
<tr>
<td>Do you distinguish between governmental and private use?</td>
<td>n/a</td>
<td>No, it is distinguished by finality principle not by data processor category. The CNIL can’t formally forbid biometrics in the private sector.</td>
</tr>
<tr>
<td>Re biometric storage- do you favour centralised storage or on a card or another token?</td>
<td>Storage under the control of the user – although it will depend to some extent on the application. Some central storage may be needed if only to replace the data if they are under the control of the user on a token and the token is lost.</td>
<td>The French DPA expressed in 2001 an orientation in favour of storage under user control (i.e. the much better) but not necessary in any case.</td>
</tr>
<tr>
<td>Do you consider biometric data as personal data or even sensitive data in the sense of Article 6 EU-Data Protection Directive 95/46/EG? If yes, are there specific conditions on the processing of those data according to your country’s regulations?</td>
<td>We consider biometric data to be personal data (they enable an individual to be identified). We consider them to be sensitive data even if they are sometimes capable of revealing health, race, ethnic origin etc. Specific conditions for the processing of sensitive personal data are included in Schedule 3 of the Data Protection Act.</td>
<td>The law draft translating the directive (and after a first lecture in lower chamber) expressed that biometrics is sensitive data in the directive sense. Until now, only biometrics in the public sector can formally be forbidden by the CNIL.</td>
</tr>
<tr>
<td>DOES IT MAKE A DIFFERENCE WHETHER BIOMETRIC RAWDATA OR TEMPLATES ARE STORED, USED, PROCESSED OR TRANSFERRED?</td>
<td>Presumably templates are less likely to reveal sensitive personal data than raw biometric data but they will both be personal data if they are stored in an electronic format or even as part of structured manual records.</td>
<td>No, because you can always identify people with a template! (the purpose of biometrics, isn’t it ?).</td>
</tr>
<tr>
<td>ARE THERE ANY LICENSES, LIMITATIONS OR BEST PRACTICES IN USE IN TERMS OF MANUFACTURING AND OPERATING BIOMETRICS? IF YES, PLEASE DESCRIBE WHICH ONES AND FOR WHICH</td>
<td>Not aware. The biometrics industry are best placed to answer this question.</td>
<td>There are no Best Practices in France (the CNIL’s recommendations apart).</td>
</tr>
<tr>
<td>APPLICATIONS/OPERATORS.</td>
<td>Are you aware of any current usage of biometrics in your country? If yes, please describe in which applications (gov./private) and with which goal (positive or negative identification/verification). Do you have any objections against a special kind of use? Why/why not?</td>
<td>There are undoubtedly many applications in the field of security/access control. Facial recognition is used in conjunction with CCTV in some applications. Fingerprints are used widely in the criminal justice system. We are aware of an application where fingerprints are used in a school to control the issuing of library books. There is a trial system at Manchester Airport using hand geometry to control staff access. There has also been a government consultation on the possible introduction of an entitlement card (identity card) in the UK. This could incorporate a biometric (at the moment it is far from certain that the proposed card will ever see the light of day). In some applications it is simply disproportionate to use a biometric e.g. the issue of library books to children. Biometrics should be declared at the CNIL (for both private or public sector application). The market is not specially sparkling. The most sensitive biometrics are tracks biometrics (fingerprint &amp; visage). Anyway, experiments limited in time (e.g. 2 months as recently) can be performed on consent basis, the CNIL makes an assessment of such experiments.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>DO YOU HAVE A PREFERENCE FOR CERTAIN BIOMETRICS IN TERMS OF DATA PROTECTION? IF YES, WHICH ONE, AND WHY?</td>
<td>From a data protection point of view the best biometrics are probably those that cannot easily be captured without the individual knowing, those which the individual does not leave behind unwittingly and those which are least susceptible to false negatives/positives. This tends to suggest techniques such as iris or retina scanning. But user acceptance is far from clear. Tracks biometrics should be reserved for high security purposes.</td>
<td></td>
</tr>
<tr>
<td>DO YOU SUGGEST ANY PROCEDURES IN USING BIOMETRICS NOT ONLY IN A PRIVACY FRIENDLY BUT ENHANCING WAY, FOR INSTANCE PREFERABLY OR EXCLUSIVELY ANONYMOUS OR ENCRYPTED?</td>
<td>No, not beyond suggesting that wherever possible identifiable information is anonymised. A process which makes use of biometrics (personal data) cannot truly be described as anonymisation. It can though be preferable to hold a biometric to link information about an individual rather than use information that reveals more about the individual (pseudonymisation). We have not seen so much privacy friendly products. It is difficult to rule such products in the law context of our DPA.</td>
<td></td>
</tr>
<tr>
<td>WHAT DO YOU THINK OF THE “PRIVACY”</td>
<td>Biometrics can be used either to enhance privacy or to erode it. We support the use of privacy. It is a necessity but PETs are a pretty fuzzy concept sometimes misunderstood. Biometrics will be</td>
<td></td>
</tr>
<tr>
<td><strong>ENHANCING TECHNOLOGIES”- CONCEPT IN TERMS OF BIOMETRICS?</strong></td>
<td><strong>We support the use of privacy enhancing technologies. Biometrics can make an important contribution to these (for example pseudonymisation) to above or improving the security surrounding personal data.</strong></td>
<td><strong>misunderstood. Biometrics will be successful economically and socially only if they are user friendly in the data protection sense.</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Is the use of biometrics approved with regard to electronic signatures? Are there any specific regulations in terms of biometrics within electronic signatures?</strong></td>
<td><strong>As far as we know there aren’t any specific regulations. We haven’t given any particular thought to this from a data protection point of view and</strong></td>
<td><strong>There are no regulation in France for such a combination. If it would be, it should be made by the French BSI.</strong></td>
</tr>
<tr>
<td><strong>Have you made any statements on biometrics that are available and you can add to your replies?</strong></td>
<td><strong>no</strong></td>
<td><strong>no</strong></td>
</tr>
</tbody>
</table>
Albrecht, Astrid: Biometrie, digitale Signatur und elektronische Bankgeschäfte zum Nutzen für Verbraucher, AgV-Studie 1999 (available only in German, but see www.vzbv.de for Consumer and Privacy assessment in English)


Bromba, Manfred, On the reconstruction of biometric raw data from template data, [http://manfred.bromba.bei.t-online.de/biometrics/temppriv.htm](http://manfred.bromba.bei.t-online.de/biometrics/temppriv.htm) (02.06.2003)


CEN/ISSS Initiative on Privacy Standardization in Europe, Draft Final Report, 30 November 2001


Die Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 63. Konferenz vom 07.03.-08.03.2002: Biometrische Merkmale in Personalausweisen und Pässen, @ www.bfd.bund.de


Nanavati, Samir/Thieme, Michael/Nanavati, Raj: Biometrics – Identity Verification in a Networked World, Wiley Tech Brief Canada 2002


Papakonstantinou, Vagelis: Self-Regulation and the Protection of Privacy, Frankfurter Studien zum Datenschutz, hrsg. von Prof. Dr. Dr. hc. Spiros Simitis, Nomos Baden-Baden 2002


Petermann, Th./Sauter, A., Biometrische Identifikationssysteme, Sachstandsbericht, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (Hrsg.), TAB Arbeitsbericht Nr. 76, Berlin Februar 2002 (english summary @ www.tab.fzk.de/en/projekt/zusammenfassung/Textab76.htm)


Rejman-Greene, Marek: Privacy issues in the application of biometrics: a European perspective, submitted to Biometric Systems: Technology,
Whereas the USA has a long tradition of Codes of Conducts and Best Practices in the context of self-regulation, in Europe it is not that traditional. Thus, the first initiatives on Best Practices on Biometrics were undertaken by different institutions in the USA and Canada.

Some of the examples are:

- International Biometric Industry Association (IBIA): Privacy Principles 1999
- International Biometric Group (IBG): BioPrivacy Initiative 2001
- Information and Privacy Commissioner Ontario, Canada: Minimum Privacy Requirements for Biometrics, 1996 until today.

I Biometric Blueprint

The so called Biometric Blueprint uses the principle of Code of Fair Information Practice for biometrics and suggests basically adopting the principles of limitation of purpose, specific rights of the data subject and duties of the data controller. The US Code of Fair Information Practices (CFIP) as of 1973 is a private scheme for processing personal data (http://www.ftc.gov/reports/privacy3/priv-23.htm (31.01.2001) and contains under others:

- no covert obtaining of biometric data but announcement to the data subject when his/her data are obtained
- access to own data and right of correction
- informed consent
- scope limitation
- liability/accountability of the operator according to private and public rules (civil and criminal law)
- control of performance in order to protect integrity and authenticity of biometric data, e.g. by means of physically protected access to databases and entire IT-systems

• option of encryption
• control by an independent (federal) institution/agency respectively
  establishment of an independent private organisation to control if private self-
  regulations are observed.

II International Biometric Industry Association IBIA, USA

IBIA states that the reason for setting up IBIA Privacy Principles was to achieve
protection of biometric data in all applications, promotion of self-regulation of the
industry and contribution to transparency and clarity.

IBIA Privacy Principles:

1 Biometric data is electronic code that is separate and distinct from
   personal information, and provides an effective, secure barrier against
   unauthorized access to personal information. Beyond this inherent
   protection, IBIA recommends safeguards to ensure that biometric data
   is not misused to compromise any information, or released without
   personal consent or the authority of law.

2 In the private sector, IBIA advocates the development of policies that
   clearly set forth how biometric data will be collected, stored, accessed,
   and used, and that preserve the rights of individuals to limit the
   distribution of the data beyond the stated purposes.

3 In the public sector, IBIA believes that clear legal standards should be
   developed to carefully define and limit the conditions under which
   agencies of national security and law enforcement may acquire, access,
   store, and use biometric data.

4 In both the public and private sectors, IBIA advocates the adoption of
   appropriate managerial and technical controls to protect the
   confidentiality and integrity of databases containing biometric data.

III International Biometric Group approach

The International Biometric Group (IBG), USA, is working for several years now
also on the privacy impacts of biometrics and tries to provide their clients with an

15 Source (last modified: October 23, 2000) http://www.ibia.org/privacy.htm (as of
   19.01.2003)
16 Source: Samir Nanavati, Michael Thieme and Raj Nanavati: Biometrics – Identity
assessment of the privacy impact of specific biometric systems. IBG sees mainly four sections of impacts of biometrics on a “privacy continuum”:

1. privacy invasive: without individual knowledge or consent, link personal information from various sources, creating individual profiles; regulation required
2. privacy neutral: lacking any special precautions or design elements to ensure privacy, but also incapable of being used in a privacy-invasive fashion
3. privacy sympathetic: incorporate special design elements and controls to ensure that the biometric data cannot be used in a privacy-invasive way; make misuse very unlikely; encryption, multiple administrators, biometric data stored independently from personal data
4. privacy protective: usage of biometric authentication to protect other personal information that may be susceptible to compromise (e.g. at the workplace when employees are required to use biometrics to access sensitive files); accessing bank accounts, medical data, other personal files through biometric authentication, as opposed to PIN and passwords, because biometrically secured makes it less likely to be compromised.

They consider two categories of privacy when biometrics is used, with the first being the more critical:

1. Informational Privacy: Unauthorized collection, storage and usage, disclosure; unnecessary collection; Function Creep
2. Personal privacy: Inherent discomfort individuals may feel when encountering biometric technology.

Biometric data here is seen always as personal data including in template form as they believe that as biometric data is derived from an individual’s behavioural or physiological characteristic, and is used to verify or determine a person’s identity.

“BioPrivacy Impact Framework”:

Lower Risk of privacy invasiveness versus greater risk
Criteria:
Overt – covert (awareness of the user)
Opt-in – mandatory (system)
Verification – identification
Fixed duration – indefinite duration
Private sector – public sector (deployment)
Individual/customer – employee/citizen (capacity of the user)
User – institution (owner of the biometric information)
Personal storage – template database (place of storage)
Behavioural – physiological (type of biometric technology)
Template – identifiable data (type of data being stored)
Scope and Capabilities

1. Scope Limitation. Biometric deployments should not be expanded to perform broader verification or identification-related functions than originally intended. Any expansion or retraction of scope should be accompanied by full and public disclosure, under the oversight of an independent auditing body, allowing individuals to opt-out of system usage if possible.

2. Establishment of a Universal Unique Identifier. Biometric information should not be used as a universal unique identifier. Sufficient protections should be in place to prevent, to the degree possible, biometric information from being used as a universal unique identifier.

*Universal unique identifiers facilitate the gathering and collection of personal information from various databases, and can represent a significant threat to privacy if misused.*

3. Limited Storage of Biometric Information. Biometric information should only be stored for the specific purpose of usage in a biometric system, and should not be stored any longer than necessary. Biometric information should be destroyed, deleted, or otherwise rendered useless when the system is no longer operational; specific user information should be destroyed, deleted, or otherwise rendered useless when the user is no longer expected to interact with the system.

*This also applies to templates generated during comparison attempts, such as a template generated in the verification stage of a 1:1 application.*

4. Evaluation of Potential System Capabilities. When determining the risks a specific system might pose to privacy, the system's potential capabilities should be assessed in addition to risks involved in its intended usage.

*Few systems are deployed whose initial operations are manifestly privacy-invasive. Instead, systems may have latent capabilities, such as the ability to perform 1:N searches or the ability to be used with existing databases of biometric information, which could have an impact on privacy. Although systems with the potential to be used in a privacy-invasive fashion can still be deployed if accompanied by proper precautions, their operations should be monitored: the maximum protections possible should be taken to prevent internal or external misuse.*

5. Collection or Storage of Extraneous Information. The non-biometric information collected for use in a biometric verification or identification system should be limited to the minimum necessary to make identification or verification possible.

*In most systems, personal information will already exist independently of the biometric information, such that there is no need to collect personal information again.*
6. Storage of Original Biometric Data. If consistent with basic system operations, biometric data in an identifiable state, such as a facial image, fingerprint, or vocal recording, should not be stored or used in a biometric system other than for the initial purposes of generating a template. After template generation, the identifiable data should be destroyed, deleted, or otherwise rendered useless.

This is to prevent the storage of fingerprints and facial images as opposed to finger-scan and facial-scan templates.

Data Protection

7. Protection of Biometric Information. Biometric information should be protected at all stages of its lifecycle, including storage, transmission, and matching.

The protections enacted to protect biometric information may include encryption, private networks, secure facilities, administrative controls, and data segregation. The protections that are used within a given deployment are determined by a variety of factors, including the location of storage, location of matching, the type of biometric used, the capabilities of the biometric system, which processes take place in a trusted environment, and the risks associated with data compromise.

8. Protection of Post-Match Decisions. Data transmissions resulting from biometric comparisons should be protected. Although these post-comparison decisions do not necessarily contain any biometric data, their interception or compromise could result in unauthorized access being granted to personal information.

This protection is especially important in non-trusted environments such as the Internet.

9. Limited System Access. Access to biometric system functions and data should be limited to certain personnel under certain conditions, with explicit controls on usage and export set in the system.

Multiple-user authentication can be required when accessing or exposing especially sensitive data. Any access to databases which contain biometric information should be subject to controls and strong auditing.

10. Segregation of Biometric Information. Biometric data should be stored separately from personal information such as name, address, and medical or financial data.

Depending on the manner in which the biometric data is stored, this separation may be logical or physical.

11. System Termination. A method should be established by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking can be depopulated and dismantled.
The responsibility for making such a determination may rest with an independent auditing group, and would be subject to appropriate appeals and oversight.

User Control of Personal Data

12. Ability to "Unenroll". Individuals should, where possible, have the right to control usage of their biometric information, and the ability to have it deleted, destroyed, or otherwise rendered unusable upon request.

This Best Practice is more applicable to opt-in systems than to mandatory systems. In certain public sector and employment-related applications there is a compelling interest for data to be retained for verification or identification purposes, such that the option of unenrollment would render the system inoperable.

13. Correction of and Access to Biometric-Related Information. System operators should provide a method for individuals to correct, update, and view information stored in conjunction or association with biometric information.

Failure to provide a means of updating personal information is inconsistent with basic privacy principles, and may lead to increased likelihood of erroneous decisions.

14. Anonymous Enrollment. Depending on operational feasibility, biometric systems should be designed such that individuals can enroll with some degree of anonymity.

In web environments, where individuals can assume alternate identities through email addresses or usernames, there may be no need for a biometric system to know with whom it is interacting, so long as the user can verify his or her original claimed identity.

Disclosure, Auditing, Accountability, Oversight

15. Third Party Accountability, Audit, and Oversight. The operators of certain biometric systems, especially large-scale systems or those employed in the public sector, should be held accountable for system use. As internal or external agents may misuse biometric systems, independent system auditing and oversight should be implemented.

Depending on the nature of a given deployment, this independent auditing body can ensure adherence to standards regarding data collection, storage, and use.

16. Full Disclosure of Audit Data. Individuals should have access to data generated through third-party audits of biometric systems.

Biometric systems which may pose a potential risk to privacy should be monitored and audited by independent parties; the data derived from such
oversight should be available to facilitate public discussion on the system's privacy impact.

17. System Purpose Disclosure. The purposes for which a biometric system is being deployed should be fully disclosed.

For example, if individuals are informed that the a system is to be used for identity verification, it should not be used for 1:N identification. Without full disclosure of the purposes for which a system is being deployed, it is difficult to make informed assessments on the system's potential privacy impact.

18. Enrollment Disclosure. Ample and clear disclosure should be provided when individuals are being enrolled in a biometric system. Disclosure should take place even if the enrollment templates are not being permanently stored, such as in a monitoring application.

This includes employees enrolled in a facial-scan system through badge card pictures or drivers’ licenses photos, or telephone callers enrolled in a voice-scan system. Informed consent to the collection, use and storage of personal information is a requirement of privacy-sympathetic system operations.

19. Matching Disclosure. Ample and clear disclosure should be provided when individuals are in a location or environment where biometric matching (either 1:1 or 1:N) may be taking place without their explicit consent.

This would include facial-scan technology used in public areas and fingerprint information taken from employees.

20. Use of Biometric Information Disclosure. Institutions should disclose the uses to which biometric data are to be put, both inside and outside a given biometric system.

Biometric information should only be used for the purpose for which it was collected and within the system for which it was collected unless the user explicitly agrees to broader usage. There should be no sanctions applied to any user who does not agree to broader usage of his or her biometric information.

21. Disclosure of Optional/Mandatory Enrollment. Ample and clear disclosure should be provided indicating whether enrollment in a biometric system is mandatory or optional. If the system is optional, alternatives to the biometric should be made readily available.

Individuals should be fully aware of their authentication options: There should be no implication that enrollment in a given system is compulsory if it is optional.

22. Disclosure of Individuals and Entities Responsible for System Operation and Oversight. As a precondition of biometric system operation, it should be clearly stated who is responsible for system operation, to whom questions or requests for information are addressed, and what recourse individuals have to resolve grievances.
23. Disclosure of Enrollment, Verification and Identification Processes. Individuals should be informed of the process flow of enrollment, verification, and identification. This includes detailing the type of biometric and non-biometric information they will be asked to provide, the results of successful and unsuccessful positive verification, and the results of matches and non-matches in identification systems. Furthermore, in 1:N systems where matches may be resolved by human intervention, the means of determining match or non-match should be disclosed.

24. Disclosure of Biometric Information Protection and System Protection. Individuals should be informed of the protections used to secure biometric information, including encryption, private networks, secure facilities, administrative controls, and data segregation.

25. Fallback Disclosure. When available, fallback authentication processes should be available for individuals to review should they be unable or unwilling to enroll in a biometric system. These fallback procedures should not be punitive or discriminatory in nature.

© Copyright 2002 International Biometric Group

IV Minimum Privacy Requirements according to Ann Cavoukian, Consumer Biometric Applications

The Data Protection Commissioner of Ontario, Canada, has set up privacy requirements on biometrics very early in the international discussion. According to her, significant privacy protections within consumer applications are identified as:

- participation strictly voluntary
- collection only with full and informed consent
- no collection of the actual raw image of a biometric (template should be only an encrypted mathematical representation due to fear of Big Brother, function creep)
- data quality principle: accurate, complete, kept up to date
- purpose specification principle by the time of data collection: purpose to be told to data subject before collecting the data

Source: Information and Privacy Commissioner/Ontario, Privacy and Biometrics, Canada (September 1999), http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&U_ID=0&P_ID=11433 (as of 18.03.2003);
• tell consumer whether verification or identification is used; verification often suffices (main question is in most application: entitlement of the person who claims access)

• tell consumers the risks and benefits when participating/ not participating in the biometric application

• use limitation principle: proper technical and policy restrictions of the operator in place? E.g.: prohibit the use of biometric data for any reason other than verification of identity; the sale, exchange or provision of biometrics. Data to third parties (except: court order or warrant); the identification of biometrics. Data using a means other than a match with a living biometric, and the discriminatory use of biometric data

• security safeguards principle: high level security for biometric data itself by: control by its owner; limited access to biometric data to persons with a specific need; biometric data stored separately from identifying information; stored biometric data cannot be re-engineered; encryption of the template; after creation of template, no evidence of the original biometric data or raw data; system design to eliminate replay attacks; destroy all biometric data securely when no longer necessary

• openness principle: information and education; tell users about your companies’ policy and practices related to biometric systems (information handling and privacy protection practices)

• individual participation principle: specific rights of the data subject

• accountability principle: data controller accountable for complying with measures that give effect to the principles

Moreover, encryption is required. Any biometric information must be encrypted; the original biometric must be destroyed after the encryption process. The encrypted biometric information can only be stored or transmitted in encrypted form, then destroyed in a prescribed manner.

V Recent Developments

TeleTrusT Working Group 6 with its sub-working group on legal aspects of biometrics has started to further develop the BIOVISION Best Practices on national level in cooperation with the German Forum for Criminal Prevention and its legal group. The Biometrics Working Group is going to further develop this Best Practice on the level of the UK national law also in cooperation with TeleTrusT WG 6.

18 http://www.teletrust.de
19 http://www.cesg.gov.uk/technology/biometrics/
In April 2003, the Biometrics Institute of Australia has announced a successful tender for setting up a Privacy Code of Conduct in the biometrics industry to PPIB Pty. Ltd., Australia\(^{20}\). Their work has not started so far, but the BIOVISION team will exchange experiences in this area within the frame of the European Biometric Forum as continued work of the BIOVISION project.

\(^{20}\) Source: Biometrics Institute, Australia, Email: manager@biometricsinstitute.org, as of 04.05.2003