ARTICLE 29 - Data Protection Working Party

12168/02/EN
WP 80

Working document on biometrics

Adopted on 1 August 2003

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Working Document:

1. INTRODUCTION

The rapid progress of biometric technologies and their expanded application in recent years necessitates careful scrutiny from a data protection perspective[2]. A wide and uncontrolled utilisation of biometrics raises concerns with regard to the protection of fundamental rights and freedoms of individuals. This kind of data is of a special nature, as it relates to the behavioural and physiological characteristics of an individual and may allow his or her unique identification[3].

Biometric data processing is now often used in automated authentication/verification and identification procedures, in particular for the control of entry to both physical and virtual areas (i.e. access to particular electronic systems or services).

Previously, the use of biometrics was mainly confined to the areas of DNA and fingerprint testing. The collection of fingerprints was used in particular for law enforcement purposes (e.g. criminal investigation). If society encourages the development of fingerprint or other biometric databases for further routine applications, it may increase the potential re-use by third parties as an element of comparison and research in the framework of their own purposes, without such an objective having initially been sought; these third parties may include law enforcement authorities.

A specific concern related to biometric data is that the public may become desensitised, through the widening of the use of such data, to the effect their processing may have on daily life. For example, the use of biometrics in school libraries can make children less aware of the data protection risks that may impact upon them in later life.

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

2 Since 11 September 2001, biometrics has often been presented as a good means to improve public safety. In the European Union, there are discussions concerning the incorporation of biometrics on ID cards, passports, travel documents and visas. The U.S. will soon require biometric identifiers for foreigners when entering and leaving the country. The ILO Convention n° 108 was modified in 2003 in order to introduce the compulsory biometrics for seafarers. There are also discussions in other international fora like the G8, OECD etc.

3 However, the unique identification depends on different factors including the size of the database and the type of biometrics used.

The purpose of the present document is to contribute to the effective and homogenous application of the national provisions on data protection adopted in compliance with Directive 95/46/EC upon biometric systems. This paper will focus primarily on biometric applications for authentication and verification purposes. The Working Party intends to provide uniform European guidelines, particularly for the biometric systems industry and users of such technologies.

2. DESCRIPTION OF BIOMETRIC SYSTEMS

Biometric systems are applications of biometric technologies, which allow the automatic identification, and/or authentication/verification of a person[4]. Authentication/verification applications are often used for various tasks in completely different areas and under the responsibility of a wide range of different entities.

Each biometric, whether for authentication/verification or identification, is, more or less, depending on the concerned biometric:
- **universal :** the biometric element exists in all persons[5] ;
- **unique** : the biometric element must be distinctive to each person ;
- and **permanent :** the property of the biometric element remains permanent over time for each person.

One can distinguish between two main categories of biometric techniques, depending on whether stable data or dynamic behavioural data are used[6].

Firstly, there are physical and **physiological**-based techniques which measure the physiological characteristics of a person and include : fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odour detection, voice recognition, DNA pattern analysis[7] and sweat pore analysis, etc.

Secondly there are **behavioural**-based techniques, which measure the behaviour of a person and include hand-written signature verification, keystroke analysis, gait analysis, etc.

Taking into consideration the rapid technical evolution and the increased concern for security, many biometrics systems work by combining different biometric modalities of the user with other identification or authentication technologies. Some systems for instance

---

[4] The difference between authentication (verification) and identification is important. Authentication answers to the question: Am I the one I pretend to be? The system certifies the identity of the person by processing biometric data which refer to the person who asks and takes a yes/no decision (1:1 comparison). Identification answers to the question: Who am I? The system recognises the individual who asks by distinguishing him from other persons, whose biometric data is also stored. In that case the system takes a 1-of-n decision, and answers that the person who asks is X.

[5] In this respect, not all biometric elements are equivalent and the rate of distinguishing one person from another is very different, according to the type of biometrics used. The most distinctive biometric elements seem to be DNA, retina and fingerprint.

[6] Some techniques can be both physiological and behavioural.

[7] Although the use of DNA for biometric identification raises specific issues, this paper will not include a discussion of those. One can mention that the generation of a DNA profile in real time as an authentication tool seems not currently possible.

cumulate face recognition and voice registration. To perform authentication, three different methods may be used jointly – based on something an individual knows (password, PIN, etc.), something an individual owns (token, CAD key, smart card, etc.) and something an individual is (a biometric feature). For instance, with a computer, one could insert a smart card, type a password and present his/her fingerprint.

The collection of biometric samples, the so-called biometric data (e.g. image of the fingerprint, picture of the iris or of the retina, recording of the voice), is carried out during a phase called "enrolment" by using a sensor specific to each type of biometrics. The biometric system extracts from the biometric data user-specific features to build a biometric "template". The template is a structured reduction of a biometric image: the recorded biometric measurement of an individual. It is the template, presented in a digitalized form, which will be stored and not the biometric element itself. In addition, biometric data may be processed as raw data (an image) depending on the functioning of the biometric system that is used[8].

The enrolment phase plays a key role as it is the only one in which raw data, extraction and protection algorithms (cryptography, hashing, etc.) and templates are all simultaneously present. It should be stressed in this regard, that if the raw data reveal information that may be regarded as sensitive in the meaning of Article 8 of Directive 95/46/EC, then the enrolment process of such data should happen in accordance with this provision (see below point 3.7).

An additional issue that is also important from a data protection point of view is the form of the storage of users' templates. This depends on the type of application for which the biometric device will be used and the size of the templates themselves. The templates can be stored in one of the following ways:

a) in the memory of a biometric device ;
b) in a central database ;
c) in plastic cards, optical cards or smart cards. This method of storage enables the users to carry their templates with them as identification devices.

In principle, it is not necessary for the purposes of authentication/verification to store the reference data in a database; it is sufficient to store the personal data in a decentralised way. Conversely, identification can only be achieved by storing the reference data in a centralised database, because the system, in order to ascertain the identity of the data subject, must compare his/her templates or raw data (image) with the templates or raw data of all persons whose data are already centrally stored.

A further point which is crucial from a data protection point of view is the fact that some biometric systems are based on information, like fingerprints or DNA samples, that may be collected without the data subject being aware of it since he or she may unknowingly leave traces. In applying a biometric algorithm to the fingerprint found on a glass, one may be able[9] to find out if the person is on file in a database containing biometric data, and if so,

---

[8] This paper refers basically to biometric systems based on templates and could also be applied to raw data. However, the specificity of raw data may lead to adapted data protection requirements.

[9] However, this implies at least certain means as the ability to collect the fingerprint from the glass without damaging it, the technical equipment to process the data from fingerprints, the access to the constructor's algorithm and/or to the fingerprints database.

who he is, by proceeding with a comparison of the two templates. This also applies to other biometric systems, such as those based on keystroke analysis or distance facial recognition, on account of the specific features of the technology involved[10]. The problematic aspect is, on the one hand, that this data collection and processing may be performed without the knowledge of the data subject and on the other hand that regardless of their current reliability, these biometric technologies lend themselves to blanket utilisation on account of their "low-level intrusiveness". Therefore, it seems necessary to lay down specific safeguards in respect of them.

3. APPLICATION OF PRINCIPLES OF DIRECTIVE 95/46/EC

3.1. Application of Directive 95/46/EC

Article 2 a) of Directive 95/46/EC defines “personal data” as “any information relating to an identified or identifiable natural person (…) ; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental (…) identity”. Recital 26 adds the following explanation “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”.

In accordance with this definition, measures of biometric identification or their digital translation in a template form in most cases are personal data[11]. It appears that biometric data can always be considered as "information relating to a natural person" as it concerns data, which provides, by its very nature, information about a given person. In the context of biometrical identification, the person is generally identifiable, since the biometric data are used for identification or authentication/verification at least in the sense that the data subject is distinguished from any other[12].

According to Article 3, §1 of Directive 95/46/EC, the data protection principles apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. The directive does not apply if the data are processed by a natural person in the course of a purely personal or household activity. Many biometric applications in domestic use will fall under this category.

Beyond these specific exclusions, processing of biometric data may only be considered lawful if all the procedures involved –starting from enrolment- are carried out in respect of the provisions of Directive 95/46/EC.

---

[10] See point 3 about the application of Directive 95/46/EC and in particular point 3.3. about the obligation to inform the data subject.

[11] In cases where biometric data, like a template, are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject, those data should not be qualified as personal data.

[12] The identifiability of the person also depends on the availability of other data which –jointly or separately- allows the person in question to be identified. The possibility of "direct identification" by means of "one or more factors specific to his physical identity" is expressly mentioned in the definition of personal data of Article 2a of Directive 95/46/EC.

This paper does not cover all the issues raised by the application of Directive 95/46/EC to biometric data. Rather, only the most relevant ones are covered and therefore, it does not provide an exhaustive view of the consequences of the application of Directive 95/46/EC.

3.2. Principle of purpose and proportionality

According to Article 6 of Directive 95/46/EC, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (purpose principle).

The respect of this principle implies firstly a clear determination of the purpose for which the biometric data are collected and processed. Furthermore, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way. Proportionality has been the main criterion in almost all decisions taken until now by the Data Protection Authorities on the processing of biometric data.[13]

For access control purposes (authentication/verification), the Working Party is of the opinion that biometric systems related to physical characteristics which do not leave traces (e.g. shape of the hand but not fingerprints) or biometrics systems related to physical characteristics which leave traces but do not rely on the memorisation of the data in the possession of someone other than the individual concerned (in other words, the data is not memorised in the control access device or in a central data base) create less risks for the protection for fundamental rights and freedoms of individuals[14]. Several Data Protection Authorities have endorsed this view stating that biometrics should preferably not be stored in a database but rather only in an object exclusively available to the user, like a microchip card, a mobile phone, a bank card[15]. In other words, authentication/verification applications which can be carried out without a central storage of biometric data should not implement excessive identification techniques.

Therefore, the Working Party thinks that the use of other types of application (i.e. based on digital fingerprints templates in the terminal or a central data base) should be carefully assessed before such applications are put in place. However, if this type of system is going to be implemented, for instance in cases such as high security installations[16], it may be considered to be data processing which presents risks as per the meaning of Article 20 of Directive 95/46/EC and may need to be submitted to prior checking by the data protection authorities in accordance with national law (see point 3.5).

---

13 Decisions for instance of the Dutch, French, German, Italian and Greek Authorities.

14 One may distinguish biometric data that are processed centrally from the case where reference biometric data are stored on a mobile device and the matching process happens on the card but not on the sensor or even when the sensor is also part of the mobile device.

15 The mechanisms put in place to solve the problems resulting from lost, stolen or damaged cards must be taken into account and those not leading to the storage of biometric data should be promoted. Whenever feasible, the data should be collected once again directly from the data subject.

16 Such is the current state of biometric technology that reliable, real-time pure identification solutions for a population of any real size do not yet exist, and it is not likely that any will be available in the foreseeable future.

Directive 95/46/EC prohibits further processing that would be incompatible with the purpose for which the data was collected. For instance when biometric data are processed for access control purposes, the use of such data to assess the emotional state of the data subject or for surveillance in the workplace would not be compatible with the original purpose of collection. All measures must be taken to prevent such incompatible re-use[17]. Directive 95/46/EC provides for exemptions to the prohibition to further process data for incompatible purposes but specific conditions apply.

It is generally accepted that the risk of the reuse of biometric data obtained from physical traces unknowingly left by individuals (i.e. fingerprints), for incompatible purposes is relatively low if the data is not stored in centralised databases, but remains with the person and is inaccessible to a third party. The centralised storage of biometric data also increases the risk of the use of biometric data as a key to interconnecting different databases that could lead to detailed profiles of an individual's habits both in the public and in the private sector. Moreover, the question of compatible purpose raises the issue of interoperability of different systems using biometrics. The necessary standardisation for interoperability could lead to greater interlinking between databases.

The use of biometrics additionally raises the issue of proportionality of each category of processed data in the light of the purpose for which the data are processed. Biometric data may only be used if adequate, relevant and not excessive. This implies a strict assessment of the necessity and proportionality of the processed data[18]. For instance, the French CNIL has refused the use of fingerprints in the case of access by children to a school restaurant,[19] but accepted for the same purpose the use of the outline of the hand pattern. The Portuguese data protection authority has recently issued an unfavourable decision concerning the use of a biometric system (fingerprint) by a university to control the assiduity and punctuality of the non-teaching staff[20]. The German data protection authority has handed down a favourable decision on the introduction of biometric characteristics on identity papers in order to prevent their falsification, provided that the data are stored in the microchip of the card rather than in a database for comparison with the owner's fingerprints.

A specific difficulty may arise as biometric data often contain more information than that which is necessary for identification or authentication/verification functions. This is more likely to be the case concerning the original image (raw data) since the template may and should technically be constructed in a way to preclude the processing of data that are not

---

17 As stated above, this purpose must be clearly defined.

18 Moreover, anonymity or the use of pseudonyms must remain possible in certain circumstances. The mechanisms put in place to solve the problems resulting from lost, stolen or damaged cards must be taken into account in this context and those not leading to the storage of biometric data should be promoted .Whenever feasible, the data should be collected once again directly from the data subject.

19 However it seems that the UK data protection authority has accepted the use of fingerprints in similar circumstances where appropriate safeguards have been put in place.

20 The Portuguese data protection authority has been of the opinion that the application of such systems was disproportionate and excessive, considering the purpose of the data processing. The system would store this data in a biometric device and the universe of persons to be controlled was approximately 140.

necessary. Unnecessary data should be destroyed as soon as possible[21]. In addition, some biometric data may reveal racial origin or concern health. (see below point 3.7.).

Finally, it should be mentioned that the use of biometric systems might be constructed in such a way that they could be considered as privacy enhancing technology *inter alia* because they may reduce the processing of other personal data like name, address, residence etc.

3.3. Fair collection and information of the data subject

The processing of biometric data and in particular its collection should happen in a fair way[22]. The controller should inform the data subject in accordance with Articles 10 and 11 of Directive 95/46/EC[23]. This includes in particular the exact definition of the purpose and the identity of the controller of the file (who will often be the person running the biometric system or applying the biometrical technique).

Systems that collect biometric data without the knowledge of data subjects must be avoided. Some biometric systems like distance facial recognition, collection of fingerprints, tapping of the voice present more risk from this perspective.

3.4. Criteria for making data processing legitimate

The processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of Directive 95/46/EC. If consent is used as a legitimacy ground by the controller of the file, the Working Party underlines that it must respect the conditions set up in Article 2 of Directive 95/46/EC (any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to the data being processed).

3.5. Prior Checking – notification

As previously mentioned, the Working Party supports the use of biometric systems that do not memorise traces in a terminal access device nor store them in a central database (see point 3.2.). But, if it is planned that such systems are to be used and in the light of the risk of (re)use for different purposes as well as of the specific dangers in case of unauthorised access, the Working Party recommends that Member States should consider submitting them to prior checking by data protection authorities in accordance with Article 20 of Directive 95/46/EC, as this kind of processing is likely to present specific risks to the rights and freedoms of data subjects. If Member States intend to introduce prior checking in relation to the processing of biometric data, national data protection authorities should be properly consulted before such measures are introduced.

---

[21] Also relevant to support this deletion is article 6, 1, e) of Directive 95/46/EC that requires keeping personal data for *no longer* than necessary for the purposes for which data are processed.

[22] Article 6 (a) of Directive 95/46/EC.

[23] Exemptions to the obligation to inform the data subjects provided for in Articles 10 and 11 of Directive 95/46/EC should be based on legislative measures and constitute a necessary measure to restrict the scope of the obligation of information to safeguard the interests listed in Article 13 of Directive 95/46/EC (public security, prevention, investigation, detection and prosecution of criminal offences etc.).

3.6. Security measures

The controller must, in accordance with Article 17 of Directive 95/46/EC, take all appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of biometric data over a network. Security measures must be taken when biometric data are processed (storage, transmission, extraction of characteristics and comparison etc.) and in particular if the controller transmits such data via the Internet. The security measures could include for instance the encryption of the templates and the protection of encryption keys in addition to access control and protection making it virtually impossible to reconstruct the original data from the templates.

Some new technologies should be taken into account in this context. An interesting development is the possibility to use biometric data as encryption keys. This would a priori create less risk for the data subject as it may only be decoded on the basis of a new collection of the biometric data from the data subject himself and so it avoids the creation of databases containing templates of biometric data that have the potential to be reused for unrelated purposes.

The necessary security measures should be implemented from the beginning of the processing, and especially during the phase of “enrolment”, where the biometric data are transformed into templates or images. It should be understood that any loss of the integrity, confidentiality and availability features in respect of the databases would be clearly prejudicial to all future applications based on the information contained in such databases, as well as causing irretrievable damage to data subjects. For instance, if the fingerprints of an authorised individual were associated with the identity of an unauthorised individual, the latter could access the services available to the fingerprint owner, without being entitled to them. This would give rise to a identity theft, which – regardless of it being detected- would make the individual's fingerings unreliable for future applications, thereby limiting his/her freedom.

Errors occurring within biometric systems can have severe consequences for the individual and in particular the false rejection of authorised persons and the false acceptance of unauthorised persons can create serious problems on many different levels. A priori, the use of biometric data should reduce the risk of such errors. However, it might also create the illusion that the identification or authentication/verification of the data subject is always correct. The data subject may find it difficult or even impossible to prove the contrary. For instance, a system may mistakenly identify a data subject as someone who should not be allowed to take a plane or should not enter a specific country and who would have little means to resolve the problem when he is faced with such "indisputable" evidence against him. In such cases, it should be stressed once again, that any decision which legally affects an individual should only be taken after reaffirming the outcome of the automated processing in accordance with Article 15 of Directive 95/46/EC.

Finally, it should be mentioned that the use of biometrics might improve the control procedures for instance in the case of access to personal data related to third parties, for instance theft and misuse (authorisation procedures).

3.7. Sensitive data

Some biometric data could be considered as sensitive in the meaning of Article 8 of Directive 95/46/EC and in particular, data revealing racial or ethnic origin or data concerning health. For instance, in biometric systems based on face recognition, data revealing racial or ethnic origin may be processed. In such cases, the special safeguards provided by article 8 will apply in addition to the general protection principles of the Directive.

This does not mean that any processing of biometric data will necessarily include sensitive data. Whether a processing contains sensitive data is a question of appreciation linked with the specific biometric characteristic used and the biometric application itself. It is more likely to be the case if biometric data in the form of images are processed, since in principle the raw data may not be reconstructed from the template.

3.8. Unique identifier

Biometric data are unique and most of them generate a unique template (or image). If used widely, in particular for a substantial proportion of a population, biometric data may be considered as an identifier of general application within the meaning of Directive 95/46/EC. Article 8, §7 of Directive 95/46/EC would then be applicable and Member States would have to determine the conditions of their processing.

Where biometric data are intended to be used as a key to link databases containing personal data[24] particularly difficult issues may arise whenever the data subject has no possibility to object to the processing of biometric data. This may commonly occur in relations between citizens and public authorities.

In this perspective, it would be desirable that templates and their digital representations be processed with mathematical manipulations (encryption, algorithms or hash-functions), using different parameters for every biometric product in use, to avoid the combination of personal data from several databases through the comparison of templates or digital representations.

3.9. Code of conducts and use of Privacy Enhancing Technology

The Working Party encourages industry to produce biometric systems that facilitate the implementation of the recommendations contained in the present working document and if European or international standards are to be developed in this field, these should be elaborated in co-ordination with data protection authorities in order to promote biometric systems that are constructed in a data protection-friendly manner, minimise the social risks and prevent the misuse of biometric data. The Working Party would underline the importance of Privacy Enhancing Technologies (PETS) in this context in order to minimise the collection of data and prevent unlawful processing.

Furthermore, the Working Party underlines the importance of codes of conduct intended to contribute to the proper implementation of the data protection principles taking into account the specific features of the various sectors, in accordance with Article 27 of Directive 95/46/EC. Community codes may be submitted to the Working Party that will

---

[24] See also above point 3.2 on compatible re-use

determine, among other things, whether the drafts submitted to it are in accordance with the national provisions on data protection adopted pursuant to Directive 95/46/EC.

CONCLUSIONS

The Working Party is of the view that most biometric data imply the processing of personal data. It is therefore necessary to fully respect the data protection principles provided for in Directive 95/46/EC taking into account the particular nature of biometrics *inter alia* the ability to collect biometric data without the knowledge of the data subject and the quasi certainty of the link with the individual, when developing biometric systems.

A respect for the principle of proportionality which forms the core of the protection ensured by Directive 95/46/EC imposes, especially in the context of authentication/verification, a clear preference towards biometric applications that do not process data obtained from the physical traces unknowingly left by individuals or that are not kept in a centralised system. This allows the data subject to exercise better control on the personal data processed about him or her.

The Working Party intends to revisit this working document in the light of the experience of data protection authorities and technological developments linked to biometric applications. As biometric data is even at the present time being introduced for a wide range of uses in a number of different forums, future work will be necessary without delay especially in the context of employment, visa and immigration and travel security.

While the responsibility remains to be on the industry to develop biometric systems that are data protection compliant, a working dialogue, in particular on the basis of a draft code of conduct, between all interested parties including data protection authorities would be a great benefit from all perspectives.

Done at Brussels, on 1 August 2003
For the Working Party
The Chairman
Stefano RODOTÀ