Ministers' Deputies

CM Documents

CM(2005)43 22 March 2005[1]

---

924 Meeting, 20 April 2005
10 Legal questions

10.5 Consultative Committee of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data [CETS No. 108] (T-PD) -

Abridged report of the 21st plenary meeting (Strasbourg, 2-4 February 2005)

---

1. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), established under Article 18 of that Convention (CETS No. 108, hereinafter "Convention 108"), held its 21st meeting from 2 to 4 February 2005, with Ms Charlotte Marie PITRAT (France) in the chair. The agenda, as adopted by the T-PD, is set out in Appendix I.

2. Under Article 20, para. 3 of Convention 108, "after each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention". This report is accordingly addressed to the Committee of Ministers, which is invited to take note of it as a whole.

3. The T-PD adopted a progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (see Appendix II), which may be found on www.coe.int/dataprotection. It invited the Committee of Ministers to take note of this progress report.

4. The T-PD then had an exchange of views on necessary action to be undertaken in the field of the application of data protection principles to worldwide telecommunication networks, on the basis of a report prepared by Professor Yves POULLET and his team of the CRID (Research Centre – Computer Science and Law, University of Namur, Belgium). It entrusted its Bureau with the task of proposing, for consideration at its next plenary meeting, a programme of activities that may be undertaken on the basis of this report.

5. The T-PD took note with satisfaction of the success of the multilateral conference held in Prague on 14-15 October 2004 on the *Rights and Responsibilities of Data Subjects,* organised in co-operation with the Office for Personal Data Protection of the Czech Republic, that gathered together 35 members States. It noted that one of the main conclusions of the Conference was that the level of awareness among data subjects and controllers of data protection concepts and rules was still too low. The T-PD considered possible action that could be taken in order to raise awareness of data protection in the member states. It agreed on the usefulness of the preparation of a FAQ (Frequently Asked Questions) in electronic form and asked its Bureau to undertake preparations accordingly. It also proposed the organisation of a European Data Protection Day, similar to other European Days organised by the Council of Europe. This event could be launched on 28 January 2006, date of the 25th anniversary of the opening of Convention 108 for signature. On this occasion, actions could be undertaken in co-operation with interested stakeholders, such as national data protection authorities, who could organise open days. The European Commission indicated its interest in being associated with such an initiative. Therefore, the T-PD entrusted the Secretariat with the task of studying the feasibility of these proposals with a view to following them up when necessary.

6. The T-PD decided, subject to the adoption of the budget for 2006 by the Committee of Ministers, to hold its 22nd plenary meeting during the week starting on 6 March 2006 and took note of the dates of its Bureau's forthcoming meeting on 6-8 April 2005.

APPENDIX I

AGENDA

I. Opening of the meeting

II. Adoption of the agenda

III. Communication by the Secretariat:

IV. Exchange of views on major developments in the field of data protection since the 20th meeting of the T-PD (28-30 June 2004)

V. Draft progress report on the application of the principles of Convention 108 to the collection and processing of biometric data

VI. Application of data protection principles to the Internet

VII. Multilateral meeting on the rights and responsibilities of data subjects (Prague, 14-15 October 2004)

VIII. Other business

IX. Date of the 22nd meeting of the T-PD

Week of 6 March 2006

APPENDIX II

PROGRESS REPORT ON THE APPLICATION OF THE PRINCIPLES OF CONVENTION 108 TO THE COLLECTION AND PROCESSING OF BIOMETRIC DATA

FOREWORD

The progress report on the application of the principles of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108, hereinafter Convention 108) to the collection and processing of biometric data is the result of work commenced in 2003 by the Project Group on Data Protection (CJ-PD) under the aegis of the European Committee on Legal Co-operation (CDCJ) and, further to the restructuration of the data protection committees, pursued in 2004 and 2005 by the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD).

The CJ-PD received terms of reference from the Committee of Ministers to "prepare, as a matter of priority, for the attention of the CDCJ or its Bureau, a report on the impact of the data protection principles on the use of biometric data (fingerprints, iris recognition, face recognition, hand geometry, etc.) in different fields". Inspired by this goal, the CJ-PD gave mandate to a scientific expert, Mr Marcel YON, CEO of the German biometrics company Viisage Technologies AG, to prepare a study on biometrics, highlighting its technical aspects, to give the CJ-PD the necessary background for its task. The technical study should be read in connection with the present document, as it explains some of the concepts employed throughout this report.

After the merger of the CJ-PD and the T-PD in a restructured T-PD by the end of 2003, the renewed T-PD agreed to take over the activity on biometrics. It was very conscious of the complex nature of biometrics and of the necessity to adopt a position on the application of data protection to biometrics as a matter of urgency, in order to contribute to the ongoing debate and biometrics projects under way both at national and international level. For these reasons, the T-PD decided to prepare a progress report on the application of the principles of Convention 108 to the collection and processing of biometric data.

A draft progress report was prepared by a scientific expert, Mr Alexander PATIJN, Principal Legal Adviser at the Ministry of Justice of the Netherlands. The T-PD and its Bureau then worked in collaboration with the scientific expert to revise and finalise the progress report. The T-PD decided, at its 21st meeting on 2-4 February 2005, with Mrs Charlotte Marie PITRAT at in the chair, to make this progress report public in order to contribute to the debates and projects on biometrics that are currently under way in many member states of the Council of Europe and in other international fora, such as the OECD (Organisation for Economic Co-operation and Development) and the ICAO (International Civil Aviation Organisation). In turn, the T-PD welcomes contributions and feedback from interested member states or other international organisations or entities on the content of this report. In the area of biometrics, a concerted approach namely bears a special importance given the complexity of the subject and its implications for human beings.

The T-PD also wishes to draw attention to the following instruments and reports of the Council of Europe, which are of some relevance to the issue of biometrics:

Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987) and its three Evaluation Reports

Recommendation No.R(89) 2 on the protection of personal data used for employment purposes (18 January 1989) and Explanatory Memorandum

Recommendation No.R(91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991) and Explanatory Memorandum

Recommendation No.R(97) 5 on the protection of medical data (13 February 1997) and Explanatory Memorandum

Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003)

Guiding principles for the protection of personal data with regard to smart cards (2004)

Study on the introduction and use of personal identification numbers : the data protection issues (1991)

The progress report has been drafted based on the state of the arts of biometrics at the time of its preparation. If the T-PD deems it necessary in view of new developments in the field of biometrics, it may be complemented or further progress reports may be issued in the future.

The progress report contains four parts:

An introductory part

A second part that seeks to identify the specificities of biometrics

A third part that proposes criteria enabling the shaping of the architecture of biometrics systems

A fourth part that builds on the elements of parts II and III to determine how Convention 108 should be applied to biometric data. Therefore, some notions may be found both in parts II and III and in part IV.

I. Introduction

Biometrics is a traditional method of identification of individuals: fingerprints for instance have been used for decades. However, two recent converging developments currently boost the use of biometrics. Firstly, there is a growing pressure to identify individuals unambiguously in both the private and the public sector. The present worldwide terrorist threat has intensified efforts to identify persons uniquely as it is assumed that terrorists assume multiple identities. In the private sector identity fraud is an increasing problem, allowing criminals for instance to embezzle large sums of money from victims whose identity they fraudulently assume. Secondly, rapidly developing new technology seems to meet this challenge by using biometrics by automatic means, allowing for mass identity checks within seconds and on the spot with a sufficient degree of certainty.

In many countries public authorities are considering or are already in the process of including biometric data on identity documents such as passports[2]. The use of fingerprints, iris scan and face recognition are at present the most probable methods. Private companies like banks consider the issuance of smart cards with biometric data for their clients to make financial transactions. Meanwhile, even schools have begun to identify their pupils in order to deny unauthorized youngsters access to their restaurants. In the near feature, domestic applications might come to the market. These applications will have to be watched and analysed as they appear.

The application of biometrics raises important human rights aspects. The integrity of the human body and the way it is used with regard to biometrics constitute an aspect of human dignity. Therefore, in considering whether or not to apply biometrics as a solution to a specific problem, controllers should exhibit special ethical responsibility. Biometrics is in its infancy and there is yet little knowledge about possible draw-backs. Once the technique is chosen on a larger scale, an irreversible development might have been started with unforeseeable effects. The precautionary principle requires a certain reticence under these circumstances. Article 8 ECHR has particular relevance for biometrics. On the one hand the right to respect for private life implies respect for somebody's body. During the process of collection and use of bodily features, human dignity should be fully respected. Questions about handicapped people or people whose physical characteristics do not fit technical standards need to be answered. Fall-back procedures should be available in case of failure of the system if anyone's physical characteristics do not fit the technical standards. On the other hand the collection of personal data in view of their automatic processing raises specific questions of data protection, in particular as biometric data might reveal unnecessary but sometimes unavoidable sensitive data e.g. information about certain illnesses or physical handicaps.

Many reports about data protection and biometrics have recently been published.[3] The Council of Europe's *Convention for the protection of individuals with regard to automatic processing of personal data* of 1981 (Convention 108, hereafter 'the Convention') established a Consultative Committee with the task, inter alia, to give opinions on the relevance of the Convention in specific areas. The Convention gives effect to article 8 ECHR with regard to the automatic processing of personal data. It establishes general principles that aim at avoiding interference with private life or, where this unavoidable, providing safeguards. The principles do not give a straightforward answer on which concrete processing of personal data is allowed and which is not. Instead they need a translation with regard to concrete applications. Biometrics does not escape this general rule. The Committee has found that the principles of the Convention have successfully been formulated in a technology-independent way. They can be applied even though the automated processing of biometric personal data was as yet unknown when the Convention was drawn up.

It is hardly disputed that we are at the dawn of an era where people are no longer recognised and identified within relatively small communities that issue the credentials of their identity. The recent globalisation of society, together with increasing security threats and on-going development of information technology, give rise to enormous expectations of the use of biometrics for the verification (authentication) and identification of individuals. On the other hand, many fear that without due regulation rights related to the protection of human dignity and private life will be infringed without sufficient justification.

The Committee deems it necessary to draw attention to some questions on the relation between the Convention and the use of biometrics. The Convention permits the application of its rules to the manual processing of personal data. One could think of the traditional manual comparison between a photograph on a passport and the person showing it at an identity check or the cumbersome comparison, not too long ago, of

fingerprints retrieved from a crime scene with those taken from known criminals. The Committee has not specifically gone into this aspect of manual processing. It focuses on the large scale use of automatically processed biometric data for the verification of an alleged identity or the identification of persons within seconds on the spot in case of an identity check. There is yet little experience with such applications and they entail risks of abuse. Although the data themselves in general do not reveal information about the individuals that are checked, in connection with the circumstances under which they are collected the biometric data permit gaining knowledge about the data subjects that might neither be necessary for the purpose of collection nor have a proper legal basis.

The Committee refrains further from going into the aspects of supervisory authorities and transfer of biometric data to countries that do not provide adequate protection. These aspects are dealt with in the Additional Protocol to Convention 108 on supervisory authorities and transborder data flows (ETS N° 181), which has recently come into force. The general rules enshrined in it are relevant for biometric data as well. Problems specific to biometric data have not yet come to the foreground, but a further examination of this issue may prove necessary in the future.

This report is intended as guidance for all those who have to decide on the question of whether to use biometrics and, if so, what conditions and safeguards could be envisaged. The time is not ripe for final judgments. Much is still open. The perceived advantages might contain drawbacks that are not yet fully known. Some fears may turn out to be unfounded. The Committee therefore chooses to confine itself to a progress report. It does not state final conclusions but aims to contribute to the debate on the processing of biometric data and data protection. It recommends taking precautions to avoid possibly irreversible developments that are not aimed at but contain considerable and unnecessary drawbacks for the protection of personal data. The Committee intends to update this report or issue further reports or draw up new law instruments as soon as developments require it.

II. What is specific about biometrics?

Description of technicalities

'Biometrics' refers to systems that use measurable, physical or physiological characteristics or personal behaviour traits to recognise the identity, or verify the claimed identity of an individual. The system is based on the following steps. A biometric sample is taken from the individual, for instance a fingerprint or iris scan. This physical characteristic can be represented by a picture. Often data are extracted from that sample. These extracted data constitute a biometric template. The biometric data, either the picture or the template, are stored on a storage medium. These preparatory phases together are called the process of enrolment. The person whose data are thus stored is called the enrolee.

The actual purpose of a biometric system is only achieved at a later stage. If a person presents himself to the system, the system will ask him to submit his biometric characteristics. The system will then compare the picture of the submitted sample (or the template extracted from them) with the biometric data of the enrolee. If the match succeeds, the person is recognised and the system will 'accept' him. If the match does not succeed, he is not recognised and he will be 'rejected'.

The picture or the template of the enrolment will seldom be identical to the picture or the template of the biometric features that will later be presented. The relevant feature often changes slightly or is submitted in a manner slightly different from during the enrolment. Inevitably there will be a certain probability in the match. The absence of a perfect match does not exclude establishing with a sufficient degree of certainty that the person who at a latter stage submits his biometric features is the same as the one who is enrolled.

Verification and identification

To fulfil a certain purpose a choice must be made between two functions of biometrics. One function consists of verification, the other of identification.

Verification means comparing a presented biometric sample with the corresponding enrolled biometric data pertaining to one single person. It is envisaged that to enhance security sometimes more than one

biometric feature of an individual is checked, e.g. his fingerprint and his iris. In that case the system would only recognize the person if the cumulative check on both features yields a positive result. The result is yes or no, the match succeeds or does not succeed. It is irrelevant whether the enrolled data are only stored in an individual storage medium (e.g. a smart card), in a database or in both. The decisive factor is that, in the case of an identity check, the data of only a single data subject are automatically processed.

In the case of identification, the presented sample is not only matched with the enrolled data of the allegedly same person, but also with the biometric data of other data subjects in the same database or connected databases. This excludes the possibility of having the enrolled data solely stored on an individual storage medium. It implies a search to establish a possible hit between the presented sample of the individual and the enrolled data of (many) other individuals. It may thus appear that the same biometric data are attached to allegedly more individuals or that allegedly the same person is connected with different biometric characteristics enrolled in the database. This would mean that either one person uses more than one identity or someone is trying to hide his real identity under someone else's name. If so, that would constitute a case of identity fraud.

In choosing the function of verification or identification, much depends on the purpose to be served by the biometric system and the circumstances under which it is to be applied. The function must serve the purpose for which data have been collected and not amount to an overkill. The same statement would be, in legal terms : the instrument should not be disproportionate in relation to the purpose it has to serve. The choice of an identification system in cases where a verification system would be sufficient to serve the envisaged purpose needs special justification. Verification problems should not be solved by identification solutions.

The use of biometrics in the issuance of a passport, an identity card or a visa aims at establishing that the person has not already applied under another name. The feature that is to be enrolled should be compared with the data that are already in the system. This purpose of avoiding double entries entails a system of identification. After enrolment however, for the purpose of establishing whether the data subject is the rightful owner of the document, it is sufficient to verify whether the biometric data on it match with the data submitted at a later stage.

The Committee acknowledges that other purposes for checking passports might be legitimate. If the purpose is not only to check whether the user of the passport is the rightful owner, but there is an additional purpose, for instance to check whether the data subject under another name appears on a list of searched persons, then mere verification does not suffice. Checking on the biometrics database whether somebody appears on a list implies identification. This additional purpose should be made explicit in order to judge whether the chosen system of identification is necessary for this additional purpose.

Another example is the issuance of a bank card. Under normal circumstances it would be feasible to identify the person on the basis of a passport or other identity document. Assuming these documents are trustworthy, it is unnecessary to establish someone's identity in yet another way. The bank card could contain a person's biometric features in order to verify whether, whenever it is used, it is used by the rightful owner. This is done by verifying whether the biometric feature of the user matches the biometric feature on the card. It is unnecessary for this purpose to store any additional biometric data in a database in addition to the data already stored on the bank card itself.

Human dignity

Biometric data are collected or derive from the human body. Some claim that there is nothing more personal than one's own body. Collection of such data might be felt as an interference with human dignity. Some people may not care, others may experience psychological resistance against the human body being used as a source of data. Others again may resist offering a part of their body, be it a single finger, to a machine to be read. Others express their worry about the thoughtless trivialisation of the human body. The resistance may depend on individual, religious or socio-cultural differences amongst people. The attitude towards the use of the human body in biometrics might also change over time.

This does not imply that the use of biometrics cannot be justified but it puts limits to the areas in which it is applied. A controller considering whether, for a specific purpose, to use biometrics or possible alternative

measures, should balance the advantages of biometrics against the possible drawbacks. The balancing should take place before a choice is made. Simple convenience is insufficient justification for choosing biometrics. The purpose for which this instrument is called upon should justify its use. The use of biometric data should not be disproportionate to that purpose, taking into account all the relevant interests and values at stake. This report intends to highlight some of these interests.

Lifelong uniqueness

The feature identifying a person uniquely is not given by man but by nature, in principle unalterable throughout life. Whatever a person does to hide his identity, whether legitimately (e.g. *pentiti* who wish to hide from criminals) or illegitimately (e.g. criminals who wish to hide from law enforcement), biometrics will often permit lifelong identification. In the future, biometrics might be generally used to identify individuals for whatever purpose during their whole life. There are, however, exceptions that can cause problems to lifelong identification. Somebody's biometric features may change during his lifetime, e.g. by aging, surgery or an accident. A biometric system might not recognize him any longer.

Probability

It has been mentioned that with regard to biometrics two different moments are important. The first is the moment of enrolment with a view to introducing a person's biometric data into the system; the second, any subsequent gathering of biometric data submitted for matching with the first. An absolutely certain match or non-match between the enrolled data and the data subsequently submitted to the system is technically unfeasible. The use of a system based on biometric data relies inevitably on a mere statistical certainty. There is no zero default system. If the enrolled and submitted data match with a sufficient degree of probability, the data subject will be 'recognised' by the system. Biometric systems are thus inherently fallible.

The chance of a false recognition or a false non-recognition can heave serious consequences for the data subject. If, for instance, he or she would falsely be 'recognised' as appearing on a list of searched criminals, the practical effect could be that he or she has to prove his or her innocence. The false acceptance rate and the false rejection rate depend on many properties of the system, such as its quality and reliability, the enrolment process etc. The rates can be adjusted in such a way as to obtain the security level required for the purpose of the system. The efforts to prevent false results should be proportionate to this purpose.

The principle of fair processing of personal data implies informing the data subject about aspects of the processing that are relevant for him or her. The properties of biometric systems, being inherently probabilistic and therefore fallible, constitute such a relevant aspect. It is therefore incumbent on the controller to inform the data subject of this and about what the data subject can do if he or she is the victim of it. Any presumption of infallibility is erroneous.

The probabilistic character of biometric systems can have opposite effects for the data subject or the controller, depending upon the way the system is set up. Four situations can be distinguished:

(a) A system filters unwanted persons, e.g. a football stadium wants to keep out a number of known hooligans listed with their biometric data. A failure of the system will be to the advantage of the data subject. He or she is not recognized and will therefore not be filtered. The hooligan can enter the stadium.

(b) The same system 'recognizes' falsely the data subject. He or she will have problems to prove that he is wrongly labelled as hooligan.

(c) A system allows only the persons who are known, e.g. a smart card serves as a key to the holder to enter secured premises. A failure to recognize an authorized person will be to the disadvantage of the data subject if there is no fall-back procedure to allow the person to enter otherwise.

(d) The same system 'recognizes' falsely a person that in fact is unauthorized. This constitutes a security threat to the controller. In practice, this threat can be reduced to a perhaps acceptable minimum, it cannot, however, be excluded.

It is the data controller's responsibility to deal with the inherently fallibility of the biometric system he chose. It is up to him to establish the adequate degree of probability in relation to the purpose of the system, e.g. is it adequate to accept an error rate of one to ten thousand or should it be one to ten million? This will become particularly relevant for large scale applications. It is up to him to test regularly whether the system is still performing in accordance with the degree of accuracy that is needed for the purpose it has to serve.

Questions may arise about accurateness with regard to a possible secondary purpose that is incompatible with the purpose of the system. It would be contrary to the principle of proportionality to demand that a system using biometric data be more accurate than necessary for the original purpose of the system for the sole reason that in exceptional cases the data could be requested in accordance with article 9 of the

Convention for a secondary, incompatible purpose, e.g. for law enforcement. For instance, in the case of a biometric system for a specific purpose it might be sufficient to enrol a template consisting of twelve elements extracted from the original biometric sample. For the secondary, incompatible purpose a template consisting of at least fifty elements would be desirable. This exceptional incompatible use cannot justify the storage of these fifty elements. If in exceptional cases the data might be used for such secondary purposes, their limited trustworthiness should be taken into account.

Biometric data have the reputation of being highly reliable as they seem to be linked to somebody's real and physical presence and therefore inalienable. There is indeed in most systems a high probability that in using biometric data one is dealing with the right person. Nevertheless falsifications are possible. For instance fingerprints taken from a glass can be used to create in wax a similar fingerprint on a storage medium. More cumbersome is the programming of computers in order to artificially produce pictures as long as is necessary to match the template on a stolen data storage medium. That picture (e.g. imprinted in wax) can be falsely used as belonging to the stolen medium. This form of identity theft is insensitive to any encryption of the template stored on the stolen storage medium.

Eventhough biometric systems may seem reliable, there is nevertheless a danger in putting too much trust in these systems. Mass scale applications are still rare. The inherently probabilistic character of these systems implies that real mistakes will occur even when the system runs perfectly. There is little experience yet about their effectiveness, reliability and effects on private life. Even less is known about the societal effects of a more general introduction of all sorts of biometric systems, cumulatively in both the private and public sphere. This argues for a not too rapid instalment of these systems and for taking precautions. An all too enthusiast rapid introduction may entail unforeseen effects that are hard to reverse.

Depending on the circumstances, one could think of using two or more biometric features simultaneously. In theory it would seem to depend on the architecture of the system whether this increases or diminishes the risk of errors. If there is a double check on somebody's identity (e.g. the combination of fingerprint and iris), it would seem to make the system more secure. However, as errors are unavoidable, the procedure has a double chance of failing. The Committee wishes to put these questions without giving the answer. It can be assumed that final answers to some questions are only possible in the course of concrete experiments.

Interoperability

There is an understandable tendency to collect and process biometric features according to standardised procedures. It serves the interoperability of different systems. Systems that allow for interoperability recognize persons on the basis of their biometric characteristics irrespective of the controller that set up the system and irrespective of the purpose for which the data were collected. This deepens the gap between conflicting interests: the increased usefulness of biometric systems versus the threats of their being used for incompatible purposes.

It cannot be excluded that ongoing technological interoperability, in the long run, might have the practical effect that the use of certain biometric data come close to a general unique identifier[4]. An example of this is the personal identification number (PIN).[5] An aggravating circumstance would be that whereas a PIN-number can be changed during lifetime (e.g. following emigration), such a change is not necessarily envisageable with biometric data.

A new dimension is added with the recommendations of the ICAO aiming at international interoperability in order to enhance transport security in civil aviation. Without precise regulation this could easily lead to a wide dissemination of biometric data as some countries do not have legislation with regard to personal data or limit their protective legislation to their own residents. The Committee is aware of close cooperation between the Council of Europe, ICAO, OECD and the European Union to address some of these issues. It awaits the results of this work.

Biometrics as privacy enhancing technology (PET)

Biometrics can be used as privacy enhancing technology (PET). A biometric feature on a bank card prevents the use of the card by somebody other than the rightful owner. Biometrics can also be used to protect databases containing personal data against unauthorised access. If the person accessing the personal data in a database is identified by a biometric feature, it is probable that no unauthorised person is seeking access.

III. Criteria to choose the system architecture

The use of biometrics is possible in different system architectures. The systems can be distinguished with a view to relevance for the protection of personal data. From a data protection point of view several criteria seem to be relevant. At present, one can mention the picture or template approach and the way enrolled data are stored in relation to their accessibility. However, evolving technology in the near future might lead to systems and criteria that cannot yet be thought of.

The choice of whether to enrol the complete picture of a biometric feature or solely an extract of it in the form of a template refers to the principle of not collecting more data than is necessary for the purpose for which data are collected. Traditionally the fingerprints and a photograph of caught criminals are stored in order to trace them more easily in case of a relapse after conviction. They might then leave fingerprints at the crime scene or may be recognized by witnesses viewing the police photographs. The enrolment of the complete picture is necessary, as it is unknown beforehand which part of the fingerprint might be left. The picture might reveal sensitive data, like certain illnesses or physical handicaps. These data may not be necessary for the purpose; nevertheless their storage is unavoidable.

It is less evident that a complete picture needs to be stored in systems where recognition with the help of biometric data is effected by requiring during the secondary collection the co-operation of the data subject to submit the relevant biometric sample. For many purposes a sufficient degree of probability will be reached by extracting a template from the submitted feature to compare it with the enrolled one.

A further relevant point is the way the enrolled data, whether a picture or a template, are stored as it has consequences for their accessibility and possible dissemination. The architecture of a biometric system can be shaped in different ways. The first possibility is that the enrolled data can be stored solely on a secured individual storage medium, for example a smart card[6]. For verification purposes this might suffice. The necessary data are available only on the card. If the data subject looses his or her card, all the data are gone. The card is comparable with a key. Until recently it was assumed that the data subject thus keeps control over the use of the data relating to him or her. It was thought that when he or she does not use his or her card, the data cannot be accessed. The controller who established the purpose of the system, its means and the categories of data to be processed, would have no access to the data unless the data subject himself or herself submitted them to the system knowingly and willingly. A new technology makes it possible to equip a smart card to allow the contact less reading of the enrolled data stored on it. Thus the data subject loses the exclusive control over the use of his or her data. This could be compensated by additional security measures. For instance, the principle of fair processing could be given effect by informing the card holder

each time that the data are read from his card. Surreptitious reading of data, if necessary, should be specifically provided for by law including adequate guarantees against abuse. Even so, if the data subject is not within the ambit of a reader, the controller does not have access to the data.

Another way to shape the architecture of a biometric system is to store the enrolled data in a local or regional database, for instance under the sole control of the municipal authorities responsible for the issuance of a passport. The data can also be additionally stored on an individual storage medium for the data subject. Through his or her database the controller can check whether the biometric data of an applicant already exist in the system. Taking as an example the passport, the municipal authorities can check whether a local resident has perhaps already applied for a passport under another name. If there are other guarantees, this might be regarded adequate to prevent the acquisition of a double identity. Thus the German law on passports does not allow the creation of a federal database filled with biometric data originating from local passport issuing authorities. Neither can the data be automatically searched by federal authorities[7]. For some purposes it will be necessary to store the enrolled biometric data in a central database or make them accessible through interlink age to a group of related controllers[8].

The Committee noted that in different countries experiments are under way to test the architecture that balances best the needs to establish somebody's identity by verification or identification against the legal demands to protect biometric data in accordance with the principles of data protection. The Committee does not feel able to exclude the possibility that other relevant features of system architecture are or might become legally relevant from a data protection point of view.

The distinction between an individual storage medium and a database does not run parallel to the distinction between the functionalities of verification and identification. A system using the functionality of verification can either be based on the mere storage on an individual storage medium or on a database. If there is an individual storage medium, checking the single individual holding the medium is the only possibility. Although a database can be made to perform only this sort of check, there remains the possibility of checking the submitted sample for the secondary collection with the enrolled biometric data of other data subjects. The functionality might change overnight. A system for identification on the other hand implies necessarily a database in order to the check the submitted data with the enrolled biometric data of more than one individual. Implementing a database for the functionality of verification requires, however, special justification.

There may be exceptional circumstances where the ad hoc change of functionality or the ad hoc linking of separate databases may be deemed necessary, deviating from the purpose for which the system was originally set up. If so, article 9 of the Convention demands that the law describes these circumstances precisely beforehand. A procedure should further describe who is to decide whether these circumstances apply in a specific case and provide for additional guarantees, e.g. establishing the precise purpose of linkage and a periodic review. The Committee has discussed the question of whether there might be cases where there is justification for demanding that the architecture of the system incorporates the technical facility to collect more biometric or associated data or a more detailed template than is necessary for the purpose of the system. These extra data could be considered to be useful for the purpose of public safety or law enforcement. The Committee did not feel in a position to answer this question. However, it stressed that if such collection of extra data, incompatible with the purpose of the system, is considered to be necessary, this can only be based on a specific law that meets all the requirements of Article 8 paragraph 2 of the European Convention on Human Rights and the case-law of the European Court of Human Rights relating thereto, in particular as regards the requirement of proportionality.

Any database is under the risk of being hacked or the data being compromised whatever technical, organisational or regulatory measures have been taken. A hacker may cheat a system's security from outside. In the past decades many security measures that were deemed to be adequate have nevertheless been bypassed. Encryption of the processed data helps to heighten security but cannot guarantee absolute security. Personnel that is allowed access can abuse the data from within in spite of any regulation and supervision. Finally, history has shown that regimes obeying the rule of law can be succeeded by regimes that do not.

IV. How to apply Convention 108 to biometric data

When does Convention 108 apply to biometric data?

The Convention applies to the automatic processing of personal data (article 1). Personal data are defined as data that contain information about an identified or identifiable natural person (article 2, paragraph a.). There are different views as to whether biometric data constitute personal data. On the one hand it is argued that it might be impossible to identify somebody on the basis of, for example, an incomplete fingerprint. Furthermore, one could contend that biometric data as such do not necessarily reveal any information about an individual. On the other hand, the idea can be defended that biometric data by their very nature allow the identification of an individual as biometric data in general are lifelong unique to a person. Future technologies might allow easy identification where at present this might seem to be an impracticable task. The argument that biometric data would not reveal any information about the person is contradicted as this in any case is purely theoretical. The collection of biometric data can only take place under certain circumstances regarding, for example, the time and the place of their collection. These circumstances always reveal information about the data subject being the source of the biometric data.

The Committee finds it unnecessary to decide whether biometric data are personal data in themselves or whether this is only the case under certain circumstances. It is of the opinion that as soon as biometric data are collected with a view to automatic processing there is the possibility that these data can be related to an identified or identifiable individual. In those cases the Convention applies.

Who is the controller?

The controller is the person who establishes the purpose of the data, the categories of data to be collected and their use (article 2, paragraph d.). When the Convention applies, there must be somebody who is responsible for compliance with data protection rules. This person is addressed as the controller even in cases where this person only assumes the responsibility of avoiding any actual identification. In the case of biometric systems it is not always immediately evident who is the controller. For example in the case of databases with the biometric data of those to whom a passport has been issued, it might be the case that only the local passport issuing authorities have access to these data although the purpose, the categories of data to be stored and their use are all established by the legislator. In these cases the law should stipulate who is to bear the relevant responsibilities.

There might be multiple controllers, each of them bearing the responsibilities that the Convention assigns to them, e.g. in case of decentralised databases. Even more complex is the situation where, though a controller defines the system, its purpose etc., the data are only accessible to the data subject because the data relating to him or her are stored upon a smart card in his possession.

Sometimes there are sub-contractors who process biometric data on behalf of the controller. The controller's full responsibility is not diminished in any way. In the EU-directive 95/46 such sub-contractors are defined as 'processor' in article 2, under e, of that directive.

In all these complex situations it is necessary to make explicit who the controller is and to make this transparent for the data subject. The data subject has the right to know, without elaborate research, whom to address in case of alleged contraventions to the rules of data protection. It is not up to him or her in such complex cases to find out who is willing to or – after being sued – is compelled to assume responsibility.

Fair and legal processing

Personal data should be obtained and processed fairly and lawfully (article 5, paragraph a.). Fairness is a broad concept. With regard to biometric data, this implies in particular that the data subject is informed on the collection of data about him or her, unless he knows it already. The data subject must be aware of the purpose of the collection and of the identity of the controller.

In theory the first collection of biometric data (to be enrolled) will be either compulsory, on the basis of a law, or voluntary. An example of compulsory collection is the issuance by a public authority of an identity document, e.g. a passport. If there is a duty to show such a identity document on request to any official and it is prescribed that the document should contain biometric features, the data subject does not have any choice. In the area of private law, it is often assumed that biometric data are collected on a voluntary basis. It is said that the data subject has a free choice, for instance to get a bank card for withdrawing money. The Committee notices that similar systems started in the past with a free choice for the client but evolved through a mass

application and the acceptance of un-negotiable standard contracts or clauses[9] into a situation where de facto there is no longer a choice for data subjects that want to take part in ordinary life. Although there is no law obliging citizens, technology has become so pervasive that for individuals that want to take part in daily life a real choice is no longer available.

The second moment of processing of biometric data is the actual use of the system by submitting a biometric sample for the secondary collection of biometric data which are then matched with the originally enrolled data. Many biometric systems are designed to store additional data about the use of the system. These are referred to by different terms such as 'shadow data', 'traffic data' or 'associated data'. In general they indicate when and where an individual contacted the system. In this paper the term 'associated data' will further be used.

A legitimate purpose for the processing of associated data is to secure the good-functioning of the biometric system. As a side-effect somebody's behaviour may be profiled. Each time the data subject submits his or her biometric features he or she may leave more or less exact traces of where he or she was, when, for how long, with whom etc. The principle of fair processing would entail the data subject being able to know of each collection of associated data. Often it will be evident to the data subject as he or she has to submit his or her biometric data deliberately. In other cases, it is because he or she will need to be informed by the controller. Depending on the circumstances, it might be sufficient to give the information in general terms. In cases where it is not self-evident that in a concrete manner associated data are collected, the principle of 'fairness' implies that information is given to the data subject on each occasion the data are collected. The associated data should not be used for purposes incompatible with those for which they have been collected.

Purpose specification and the choice for a specific technique

Personal data must be processed for specific and legitimate purposes (article 5, paragraph b.). Together with the choice to use biometric data, the purpose of their processing must be determined and made explicit. A legitimate use of biometric data could be as part of access control to a country, protected areas or premises. A further purpose of including biometric data on passports or visas is to prevent the use of false identities, the obtaining of a second passport or the issuance of a passport to an unauthorized person. There is no exhaustive list of legitimate purposes.

Once the purposes are specified, the technical system should exclude the collection and processing of more personal data than is necessary for those purposes, whether biometric or associated data. This points to the distinction between the different techniques of verification and identification[10]. These techniques are instruments to serve these purposes. The purposes that the system should serve are relevant to the choice of whether or not to install a system for identification or for verification. The Committee cannot generally recommend choosing one or the other system. It can only recall that if a verification process suffices to serve the chosen purpose the instalment of an identification system needs special justification.

Non-excessiveness

Specific to biometric data is the possibility that they contain more data than are necessary for the purpose of verifying or identifying individuals (article 5, paragraph c.). It is possible to avoid the processing of unnecessary data by limiting the storage and use of biometric data to an extract that serves the specific purpose as well, both in the phase of enrolment and during secondary collection. The technical term for such an extract is 'template'. The extract should be made in such a way that the resulting data do not reveal more information than is necessary for the purpose of the system. In particular it should avoid any possible link with sensitive data. An example might be useful. The picture of an iris scan might reveal certain illnesses. This information is not necessary for the recognition of an individual. The template should be made in a way that it does not contain this unnecessary information.

A template can be compared to a list of key words extracted from a text where the text itself is not retained. The key words suffice to match with the key words generated after the subsequent gathering of the same text. Thus, the template extracted from the biometric picture during the secondary collection can be

matched with the enrolled template each time the system is effectively used. The notion ‘biometric data’ refers to either the biometric picture or to the template extracted from it.

From a data protection point of view, this extract has the additional advantage that the original picture of the biometric feature cannot be reconstructed as no text can be reconstructed from a list of key words. If only part of a fingerprint is found and this part does not contain all the extracted features, the person cannot be identified by means of a previously enrolled template. For the purpose of identifying possible perpetrators of criminal offences, it will be necessary to have a complete picture. For many other purposes extracts will suffice.

The notion of non-excessiveness is also relevant for the collection and storage of associated data. No associated data should be stored - and if stored not longer - than is necessary for the purpose for which they are collected. The exact purposes of processing associated data should therefore be made explicit right from the start of planning a system’s architecture.

Accurateness and probability

Personal data should be accurate (article 5, paragraph d.). It has been mentioned that probability is an inescapable element of processing of biometric data. Although all the data involved are accurate, the outcome of the processing might be false. This might need explanation.

It is unavoidable, even if the system functions perfectly, that once in a while the enrolled data and the data of secondary collection do not match. Somebody might then be falsely rejected. Likewise, the system might establish the similarity between the two features although they belong to different persons. Somebody is then falsely accepted.

It has been mentioned that biometric data are in general lifelong unique (cf. para 28). Exceptions are possible. People growing older may change biometric features. Illnesses, accidents or surgery may lead to a change of relevant biometric features having the effect that the biometric system fails to function well with regard to the specific data subject. The enrolled data can no longer be regarded to be accurate in view of the purpose they have to serve.

If the data do not or no longer meet the appropriate degree of exactness or similarity, the data subject’s request for rectification ought to be granted.

Preservation of data

Personal data should not be preserved for longer than is necessary for the purpose for which they have been collected (article 5, under e). For biometric data this requirement does not seem to be very problematic. As long as the system fulfils its purpose, the enrolled biometric data will be kept on one storage medium or another. Article 5, under e, mentions in general the possibility to preserve data in a such a form that the data subject can no longer be identified. With regard to biometric data the option of making the data anonymous is not available as biometric data, by their very nature, form an instrument to identify individuals, particularly when they are automatically processed.

The data of the secondary collection will be of no use once they have been compared with the enrolled data. In principle they will not be stored but deleted immediately. The storage of the data submitted for the secondary collection could only be justified in exceptional cases where reasonable grounds for suspecting identity fraud exist.

More problematic might be the question of the preservation of associated data (see para 57). They may serve different purposes. To protect highly secured areas, e.g. a nuclear plant, it might be a legitimate part of the system to know exactly who entered certain areas, when and for how long. These data serve this primary purpose. Other systems may serve another purpose, e.g. to establish whether the owner of an identity document is the rightful owner. These data may be needed to check whether the system as a whole functions well. One could think of a design that automatically gives a signal if the same biometric data are used within a short period in geographically remote areas. This may hint at a double entry, perhaps fraud. Such secondary

purpose could be deemed compatible with the original purpose. Article 5, paragraph b. allows the preserving of associated data for such secondary purposes. In both cases of primary and secondary use, the system design should specify and make explicit the duration of preservation of the associated data in relation to the purpose for which they are to be collected. The preservation of associated data for purposes that are incompatible with the purpose of collection is not allowed. A derogation is only possible if the requirements of article 9 are met.

Sensitive data

Biometric data may reveal illnesses or racial origin. Article 6 defines these as 'special categories of data' demanding appropriate safeguards. In the doctrine of data protection these data are referred to as sensitive data. New developments may lead to possibilities to infer more information from biometric data than ever imagined. In general, this new information will not be relevant to the purpose for which the data have been collected. The Committee acknowledges that under such circumstances the processing of biometric data implies the unavoidable processing of unnecessary data, comparable to the situation where a simple name reveals ethnic origin. The choice of data to be extracted in generating a template should avoid revealing sensitive data as, in general, these data will not be able to verify the data subject's identity or identify him or her. The precautionary principle demands that where new techniques may uncover unexpected new information one should be reticent to start with systems where there can be reasonable doubt that in the long run unwanted and possibly irreversible side effects may appear.

Data security

Article 7 deals with the duty to provide appropriate security measures to protect personal data. Standards for the quality of software and hardware could be established by the industry particularly in relation to large scale applications and in systems that demand a high level of security. Data protection authorities should stipulate that the technical standards include the necessary aspects related to the application of the Convention. The training of the personnel using the system and the equipment are other important factors. The training should include the raising of awareness of the responsibilities of the personnel when operating the system.

Subsequently the standards and the systems applying them should be regularly audited and evaluated, if appropriate, by an independent body taking into account all the elements of the system, such as the enrolment, the stored data, the process of matching of enrolled data with the submitted sample, the error rate, the encryption of the different phases, the personnel operating it etc.

A general measure of protection, also applicable to biometric data, consists of trustworthy algorithms to extract a template from a biometric picture and to compare the enrolled data with the subsequently submitted biometric data. The transparency of these algorithms is presently under discussion, *inter alia* in view of their interoperability. The use of encryption is recommended during the enrolment process to prevent non-authorised people having access to the raw data and thus being able to use them to impersonate the rightful user. Strong encryption of biometric data during the enrolment process, for storage and transmission over telecommunication lines enhances security and makes the unauthorised use of biometric data more difficult. Anybody who would intercept the encrypted signal, not disposing of the encryption key, should not be able to reconstruct a signal to which the biometric system would respond.

Transparency

The existence of a system using biometric data, the purpose of the system and the identity and residence of the controller should be communicated, not only to the data subject, but to the public in general (article 8, paragraph a.). Particular problems may arise with regard to the notion of purpose. It might be the case that a system serves more than one purpose, some of which are evident, while others are not. Under these circumstances, the controller should inform, on his own initiative, the data subjects and the public about the system, the purposes for which the personal data are used, the way they are used and possible risks. In other cases the principle of transparency can be served by giving information upon request.

Any derogation from the transparency of all the purposes should, in accordance with article 9 of Convention 108**,** be provided for by law and should be necessary in a democratic society in the interests of, for example, public safety.

Right of access

The data subject has access to the biometric data about him or her (article 8, paragraph b.). This right extends to the biometric data themselves as well as to the associated data that reveal - intentionally or unintentionally - information about him or her. A data subject might have an interest in checking the biometric data that the system links to his or her identity as it cannot be excluded that they have deteriorated or been falsified, yielding false rejections. The biometric data belonging to his name have to be searched on his or her request.

The data subject might claim that the enrolled biometric data or template do not or no longer adequately represent the biometric data that he or her submits on each occasion he or she uses the system, resulting in a higher rate of false rejections than average. This might be the result of biometric features changing as the data subject ages, of surgical interventions or of accidents, leading to a lasting change in the relevant biometric features. The Committee thinks that the right of access implies that such a claim be checked. The data subject does not need to present a probable cause.

The data subject has the right of access to his or her data in an 'intelligible form'. Granting the right of access to biometric data will often imply that a machine able to read the biometric data should be available. Similarly an expert may be required to interpret and check the data. The Committee believes that the controller cannot simply deny such requests by stating that a machine or an expert is not available.

The Committee discussed the possibility of an abusive exertion of the right of access. To a certain extent article 8, paragraph b. deals already with this. Unreasonably frequent requests for access can be rejected as only requests 'at reasonable intervals' must be granted. Other forms of abusive requests can also be imagined. The Committee considered that general principles of law, not limited to the field of data protection, deal with the doctrine of abuse in the exertion of rights or legal claims.

In certain cases, where there is reasonable cause to suspect identity fraud, the data controller should do his best to investigate the situation.

In practice this search can only be done to the extent that the controller himself has access to the biometric data. It is possible that this is not the case (cf. § 3 about the storage of data on a smart card) but the data subject can present a probable cause that somebody else fraudulently uses his or her biometric data in relation to the system. The Committee is of the opinion that the controller should then take the necessary measures to secure the accuracy of the data. One could think of the use of associated data to detect the alleged fraud.

Right of rectification and erasure

Biometric data or associated data may appear to be incorrect. The data subject can claim their rectification or erasure (article 8, paragraph c. of the Convention).

Whether data are correct or not has to be judged against the background of the purposes for which they have been collected. If the data are used solely to grant access to premises without the subsequent storage of associated data related to individuals, a controller could legitimately accept a greater degree of probability of a false acceptance or a false rejection, e.g. to prevent the system becoming disproportionately expensive.

The degree of probability plays a role both in the enrolment procedure and in the subsequent use of the system. During the enrolment the algorithm to extract the template from the biometric feature can be more or less extensive depending on the purpose of the system. A less extensive algorithm will increase the probability of false acceptances or rejections as the template will be less specific. In subsequent use the system can be tuned to allow a more or less strong coincidence between the enrolled picture or template with the presented biometric data. The Committee is of the opinion that it is primarily up to the controller to establish the necessary degree of probability that the system allows for. The data subject cannot claim full certainty but as much as is technically possible.

The inherently probabilistic character of the use and match of biometric data makes it unavoidable that once in a while associated data are linked to the wrong data subject. As this might be the case, the interpretation of these data with regard to an individual should take this fact into account. As a match (acceptance) or a non-match (rejection) never yields full certainty, neither can the associated data be linked to a specific data subject with absolute certainty. The same degree of probability remains throughout.

This raises special problems in systems where the data are used to systematically control somebody's behaviour, which could be justified for instance in a highly secure area where it is necessary to know who was where, when and for how long. This demands a higher degree of accuracy of the system. With regard to biometric data this means that there should be relatively little probability of a false acceptance or false rejection.

The certainty of the 'recognition' of the data subject should not be taken for granted. Nor can the data subject claim that they should be fully certain. A corollary seems to be that if inaccurate associated data are found, this does not necessarily imply that the controller has acted illegally, thus giving ground for indemnification.

Linked to the right of rectification is the right of erasure, in the case of biometric data being stored contrary to the law.

With regard to biometric data, conflict could arise between the controller and the data subject about the acceptable degree of probability of false rejections. If the data subject requests a new enrolment, although the controller does not acknowledge that the data are inaccurate, the right of rectification could be assumed to entail in principle the data subject's right to a new enrolment without excessive costs. The same holds true if the enrolled data were originally correct but the biometric feature has changed by aging, an accident or surgery. With the lapse of time the data gradually may have become incorrect.

Effective remedy

Everybody has the right to an effective remedy where the right to transparency, to access, to rectification or erasure is not met (article 8, paragraph d.). With regard to biometric data, a further specification of this right could be thought of. Several references have been made to the fact that the probabilistic character of the use of biometric data entails specific problems with regard to data protection. The choice for the use of a biometric system is the controller's risk. It is not up to the data subject to bear the possible drawbacks of such systems. Depending on the circumstances, the data subject should have the possibility of an immediate remedy being sought or have, as soon as possible, access to a review.

Somebody might not be 'recognized' by a biometric system. This can have several causes, such as the following:

(a) The person is not the same as the one whose biometric data are enrolled. The result is correct. The data do not match and the system rejects the data subject.

(b) The system's enrolled biometric data are wrong. The data should be rectified.

(c) The enrolled data are right but the secondary collection does not function well so the matching of biometric data does not succeed. The machine should be adjusted.

(d) The system works perfectly well and the data are accurate; nevertheless the probabilistic character of the matching operation leads to the result that the system does not find a match.

Other cases can be thought of also, where somebody is 'recognized'. The match between submitted data with the originally enrolled data might wrongly be indicated as successful. This might imply that the data subject is recognized as appearing on a list of unauthorized persons whereas the opposite is the case.

In all these situations an individual should, upon request, obtain a review. In case (a) the rejection will be confirmed. In all the other cases, the automated outcome should be corrected. In the end the data subject ought to

have recourse to a human being who on behalf of the controller decides whether the data subject is to be rejected or accepted[11]. The procedure for this recourse should not be disproportionately burdensome for the data subject. The same applies to persons who cannot use the system because of a physical handicap. Somebody missing both hands cannot be allowed in by a system that works on the basis of fingerprints. The controller should ensure that these persons dispose of an alternative procedure without compromising the security level which is being aimed at.

In the eventuality that the data subject and the controller have a lasting disagreement, they can address the supervisory authority under the Additional protocol to Convention 108.

The relevance of article 9 of the Convention for biometric systems

Article 9, para 2, allows for derogations to the principles mentioned above. The derogations are submitted to certain limits. The paragraph resembles article 8, para 2, of the European Convention on Human Rights (ECHR).

The gathering of personal data, whether biometric or associated data, and their subsequent processing might interfere with private life. Article 8, Para 1, ECHR, would forbid such interference unless the interference is justified in accordance with Article 8 paragraph 2. If biometric data are automatically processed the principles of Convention 108 apply, whether or not private life is at stake. The principles aim at avoiding interference with private life as much as possible. The principles apply equally to the associated data generated by the use of a biometric system as long as these data permit identification of the data subjects. Any interference with private life is only allowed if the criteria of article 8, para 2 ECHR apply. A derogation from the principles of Convention 108 is only allowed if the criteria of its article 9, para 2, apply. These criteria are similar to article 8, para 2, ECHR.

In the Rotaru vs Romania judgment of May 2000, the European Court of Human Rights decided that the secret collection of personal data for state security purposes amounted to an interference with private life. The Court therefore applied the criteria of Article 8, para 2, ECHR. In its judgment, the Court deemed necessary that the categories of persons to whom such interference applies and the data that can be collected about them should be described beforehand by law in a sufficiently precise and foreseeable manner in accordance with legitimate criteria. Sometimes it is contended that the data subject's private life is not is not interfered with as long as he or she does not notice anything. The Rotaru vs Romania judgment makes clear that this argument is not valid.

The Rotaru vs Romania judgment with regard to article 8, para 2 ECHR might have implications for the interpretation of article 9, para 2, Convention 108. The processing of biometric data and the different categories of associated personal data, the purposes of their collection and the identity of the controller should in principle be made transparent to the data subject. New technologies such as face recognition and an on-the-spot check with a list of searched criminals would constitute a form of processing without the storage of the data of all the checked persons for any longer than the few seconds necessary to perform the match. Nevertheless, it is a form of processing that would be covered by Convention 108. The surreptitious processing of these data would be contrary to the principle of fair processing and would therefore only be allowed if the criteria of its article 9 are fulfilled.

An example may illustrate this point. In spite of unsuccessful experiments so far, it cannot be excluded that in the near future it will be technically possible to identify people walking in the street by comparing their faces with a list of wanted persons. The technique is evolving to extract digitalized information from pictures in order to compare them with databases. The enrolment would consist of taking a criminal's picture after arrest. These could be matched with pictures resulting from the video surveillance of citizens walking along the street. In practice this video surveillance could be carried out secretly. As this would amount to unfair processing, this would only be allowed if the criteria of article 9 of the Convention are met. A law would be needed describing the exact ambit of the exceptions to the general rule of fair processing.

Some advocate the secondary use of associated data of existing systems using biometric data where the compatibility with the original purpose for which the data have been collected is questionable. For instance, intelligence services might be interested in preserving these data for the purpose of surveying people they deem

prone to terrorist attacks. Often this will be incompatible with the original purpose of collecting these data. Article 9 of the Convention would demand that such a measure be proved to be necessary in a democratic society for the purpose of public security. If so, the derogations to the criterion of compatibility should be laid down in a law specifying the way such data can be preserved and used for this new purpose.

Article 8, para 2, ECHR and article 9 of Convention 108 are meant as exceptions that justify an infringement to the principles enshrined in both Conventions. A limited interference with private life or a limited derogation from the rules of Convention 108 would not set aside the principles in themselves. An overall secret surveillance of the public in general, even if provided for by law, would set aside the entire principles as such and would therefore not meet the standards of either the ECHR or Convention 108.

V. Conclusions of the progress report

The Committee has had a preliminary debate on some issues of biometrics in its relation to the data protection principles as these are enshrined in Convention 108. Many questions are still open. In spite of big technological developments since the Convention was drafted, the Committee has found that its principles are still relevant also for systems using biometrics. The report reflects the relevance of the legal principles to these new techniques. It aims to contribute to the debate about the relation between human rights and biometrics that take place both at the international and national level. The Committee intends to update this report or issue further reports or draw up new legal instruments as soon as developments require it.

At this stage the Committee underlines, in particular, that:

Biometric data are to be regarded as a specific category of data as they are taken from the human body, remain the same in different systems and are in principle inalterable throughout life. They might be altered, however, for instance through aging, illnesses or surgical interventions.

Before having recourse to biometrics, the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life.

Biometrics should not be chosen for the sole sake of convenience. Human dignity might be affected by the use of biometrics. Socio-cultural aspects and possible reluctance towards the instrumental use of the human body, should be taken into account.

The biometric data and any associated data generated by the system must be processed for specific, explicit and legitimate purposes and should not be processed further for purposes that are incompatible with these.

The data should be adequate, relevant and not excessive in relation to these purposes. A technical system using biometric data should be configured to exclude the possibility to collect more biometric or associated data than is necessary for the purposes of the processing. Where templates are sufficient, the collection or the storage of the picture should be avoided.

In choosing the system architecture, the controller should balance the advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand. A reasoned choice should be made between storage solely on an individual storage medium, a decentralised database or a central database, bearing in mind the aspects relating to data security.

The architecture of a biometric system should not be disproportionate in relation to the purpose of the processing. Therefore, if verification suffices, the controller should not develop an identification solution. Biometric data that are solely used for verification purposes preferably should be stored only on a secured individual storage medium, e.g. a smart card, held by the data subject only.

The data subject should be informed about the purposes of the system and the identity of the controller unless he or she already knows, and about the personal data that are processed and the persons or the categories of persons to whom they will be disclosed as far as the information is necessary to guarantee the fairness of processing.

The data subject has a right of access, rectification, blocking and erasure of the data relating to him or her. These rights extend to the biometric data undergoing automatic processing attached to his identity, possibly associated data (such as date and place of use of the system) and to whom they have been communicated.

The controller should foresee adequate technical and organisational measures that aim to protect biometric and associated data against accidental or deliberate deletion or loss, as well as against illegal access, alteration or communication to unauthorised persons or any other form of illegal processing.

A procedure of certification and monitoring and control, if appropriate by an independent body, should be promoted, particularly in the case of mass applications, with regard to the quality standards for the software, the hardware and the training of the staff in charge of enrolment and matching. A periodic audit of the system's performance is recommendable.

If, as a result of a biometric system, a data subject is rejected, the controller should, on his or her request, re-examine the case and should, where necessary, offer appropriate alternative solutions. Procedures should be in place and made known to the data subject in the case of an allegedly false result of the system.

T-PD, February 2005

---

[1] This document has been classified restricted at the date of issue. Unless the Committee of Ministers decides otherwise, it will be declassified according to the rules set up in Resolution Res(2001)6 on access to Council of Europe documents.

[2] The EU Council Regulation 15152/04, adopted in December 2004, prescribes the introduction of biometric data in passports.

[3] The Data Protection Working Party established by Article 29 of the EU Directive on data protection issued a Working document on biometrics on 1 August 2003 on aspects relating to the Directive (www.euopa.eu.int/comm/privacy).

[4] Reference is made here to article 8 para 7 of Directive 95/46

[5] See also the Council of Europe report on *The introduction and use of personal identification numbers: the data protection issues* (1991).

[6] See the Council of Europe's "*Guiding Principles for the protection of personal data with regards to smart cards" (2004)*

[7] The European Parliament, in its opinion of 2 December 2004 on the European Commission proposal to include biometrics in the passports of EU-citizens, pleaded for a similar solution. This opinion was based on a report adopted in October 2004, in which the Committee on Liberty, Justice and Home resisted plans to establish eventually a EU-centralised database of issued passports as it would enhance the risk of incompatible use.

[8] An example is Eurodac that aims to identify refugees or alleged refugees that have applied for asylum in one of the EU-countries on the basis of their fingerprints.

[9] In French, « contrats d'adhésion »

[10] For a description of the distinction between verification and identification see under § 2, Description of technicalities.

[11] cf article 15 of the EU-directive 95/46 on the protection of personal data.