Strasbourg, 20 September 2013 T-PD(2013)06

**CONSULTATIVE COMMITTE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]**

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

**Authors**
Prof. dr. Paul de Hert
Koen Christianen LLM BSc

April 2013

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

**Commissioned by**
Council of Europe

**Concluded by**
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University

**Authors**
Prof. dr. Paul de Hert
Koen Christianen LLM BSc

April 2013

Tilburg Institute for Law, Technology, and Society (TILT)
http://www.tilburguniversity.edu/research/institutes-and-research-groups/tilt/
Telephone +31 (0)13 466 3515

# Table of Contents

1 Definition of biometrics and structure of the report ..... 5
2 The Council of Europe's 2005 progress report ..... 6
3 Recent developments within the Council of Europe ..... 9
3.1 The Council of Europe's 2011 Parliamentary Assembly report ..... 9
3.2 The Consultative Committee's modernisation work of Convention 108 ..... 13
3.3 The European Court of Human Rights: The Marper judgment ..... 14
4 Recent developments in the European Union ..... 17
4.1 Proposals of the European Commission ..... 17
4.2 European Union's Eurodac/SIS/VIS/European biometric passport ..... 18
4.2.1 Eurodac ..... 18
4.2.2 The Schengen Information System ..... 19
4.2.3 The Visa Information System (VIS) ..... 20
4.2.4 The European Biometric Passport ..... 21
5 Second generation biometrics ..... 24
5.1 What are second generation biometrics? ..... 24
5.2 Concerns about second generation biometrics ..... 24
6 Intrinsic errors of and impostor threats to biometric systems ..... 26
6.1 Intrinsic errors of biometric systems ..... 26
6.2 Risk analysis of biometric systems ..... 28
6.2.1 Introduction ..... 28
6.2.2 Impostor threats ..... 29
6.2.3 Additional threats ..... 29
6.2.4 Biometric template protection ..... 30
7 Country responses to the questionnaire ..... 32
7.1 Responses of 22 out of 47 countries ..... 32
7.1.1 Albania ..... 32
7.1.2 Austria ..... 32
7.1.3 Denmark ..... 33
7.1.4 Estonia ..... 33
7.1.5 France ..... 33
7.1.6 Georgia ..... 35
7.1.7 Hungary ..... 35
7.1.8 Ireland ..... 36
7.1.9 Italy ..... 36
7.1.10 Lithuania ..... 38
7.1.11 Macedonia ..... 39
7.1.12 Malta ..... 39

7.1.13 Monaco ..... 40
7.1.14 Montenegro ..... 41
7.1.15 Netherlands ..... 41
7.1.16 Niger ..... 43
7.1.17 Poland ..... 43
7.1.18 Portugal ..... 45
7.1.19 Romania ..... 45
7.1.20 Senegal ..... 46
7.1.21 Serbia ..... 46
7.1.22 Slovenia ..... 46
7.1.23 Switzerland ..... 48
7.2 Main results from the questionnaire ..... 49
7.2.1 Countries which have adopted legislation and regulation specifically aimed at the protection of biometric data ..... 49
7.2.2 Biometrics in the contexts of sports, school and workplace ..... 51
8 Conclusions and recommendations ..... 53
Annex A: The recommendations in the 2005 progress report ..... 58

# 1 Definition of biometrics and structure of the report

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[1] asked the authors of this report to prepare a study on biometrics including an analysis of the Member States' current regulatory framework on the protection of biometric data. The aim of this progress report is to provide an update of the Council of Europe's 2005 progress report on the application of the principles of convention 108 to the collection and processing of biometric data.[2] The authors of this report use the following definition of biometric data and biometrics:

***Biometric data (or biometrics[3]) are measurable, physiological or behavioural characteristics that can be used to determine or verify identity. Biometrics is also defined as 'the automated use of physiological or behavioural characteristics to determine or verify individuals'.*** [4]

In order to gain information on the use of biometric systems in relation to the principles of Convention 108, the 47[5] Council of Europe's Member States have been submitted a 7 questions questionnaire drafted by the authors of this report. 23 countries out of 47 Member States have provided answers to the questionnaire. Section 7.1 summarizes the answers of 22 countries because Portugal has been omitted from the report.[6] These 22 answers and the research conducted by the authors of this report will allow the Consultative Committee to form an opinion on the application of

---

[1] Convention for the protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ETS No. 108 (Convention 108), entry into force 1 October 1985, Council of Europe, available online at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[2] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (hereinafter Progress Report 2005), Strasbourg 2005, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.

[3] The plural form of biometric.

[4] This is the most accurate definition according to the authors, although numerous definitions exist. For example, the Article 29 Data Protection Working Party in 2012 suggested the following definition for biometric data: "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability", see Opinion 3/2012 on developments in biometric technologies (WP 193), issued by the Article 29 Data Protection Working Party, and adopted on 27th April 2012, available online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

Biometrics are regularly considered to be 'unique' characteristics, although this is not always the case, as DNA samples of identical twins are not unique. DNA is not immediately machine readable, therefore this type of biometric data will not be discussed in this report. All other biometrics are thought to be unique, even both eyes of the same person or the eyes of identical twins, and the fingerprints on each finger of the same individual or the fingerprints of identical twins. See Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy? Opinion* (hereinafter Irish Council for Bioethics Opinion 2009), Dublin: The Irish Council for Bioethics 2009, available online at http://irishpatients.ie/news/wp-content/uploads/2012/04/Irish-Council-Bioethics-Final_Biometrics_Doc_HighRes.pdf. The uniqueness is also considered to apply to behavioural biometrics, although further research is needed to confirm this premise.

Definitions of biometric data sometimes contain the word 'physical' or 'biological', but in this report it is omitted in favour of the word 'physiological' since the latter comprises physical, biological and chemical phenomena, see Encyclopaedia Britannica Online.

Although biometric systems are employed for several purposes (e.g. security or law enforcement), all systems have one basic function, namely authentication, subdivided into verification and identification, which are both used in the authors' definition of biometrics.

[5] Including 3 CoE members not party to Convention 108: Russia, Turkey, and San Marino.

[6] Portugal did not want its reply to be published.

the principles of Convention 108 regarding biometrics across the Council of Europe's Member States. The 7 questions of the questionnaire were:

**Question 1:** Does your country have regulation/legislation with regard to biometrics (i.e. biometric data and biometric systems)? If yes, please provide the regulation/legislation in English and in the native language.
**Question 2:** What is the state of the art of biometrics in your country? In other words, what are the latest biometric technologies?
**Question 3:** Could you please indicate what types of biometric systems are currently being used in your country and for which reasons, both in the public and the private sector?
**Question 4:** Which problems or difficulties does the public and private sector in your country encounter with regard to biometrics or the regulation/legislation regarding biometrics?
**Question 5:** Does your country have a central database for biometric data in either the public or private sector or is your country planning to set up such a database? If yes, for which purpose(s) and is it regulated?
**Question 6:** Have there been situations in your country, since 2005, in which biometric systems were hacked or compromised? If yes, please explain the situation.
**Question 7:** If, on a national level, research has been conducted regarding biometrics, please attach the report(s) of this research.

Section 7.1 contains a structured representation of the country responses.

This report firstly addresses the main findings of the 2005 progress report, including its 12 recommendations (Section 2). We elaborate on recommendations 1, 2, 5, and 8 of the 2005 report, because they remain significantly important with regard to the Council of Europe's future legal framework on the processing of biometric data. We continue our report with substantial recent developments within the Council of Europe (Section 3) and within the European Union (Section 4). Subsequently, the developments and concerns of new types of biometric technologies, the so-called second generation biometrics are discussed (Section 5). In a next section we discuss technical performances of biometric systems. All these systems encounter errors and threats (Section 6). This section also addresses biometric template protection being one possible solution to protect biometric data (Section 6.2.4). The overview of the country reports including their main results (Section 7) is followed by the general conclusions and recommendations (Section 8).

# 2 The Council of Europe's 2005 progress report

The Council of Europe's 2005 progress report on the application of the principles of Convention 108 to the collection and processing of biometric data was 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).[7] The foreword of the 2005 progress report mentions that "[The T-PD] 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

[7] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* ('Progress Report 2005'), Strasbourg 2005, p. 3, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.

the application of the principles of Convention 108 to the collection and processing of biometric data". Due to evolving technologies yielding new biometric possibilities and legal challenges the 2005 progress report needed an update.

The 2005 progress report contains 12 recommendations attached in Annex A. This section discusses the most relevant recommendations of the 2005 progress report. They require particular attention in this update of the progress report, because of the developments in biometric technology. For this reason, recommendation 1, 2, 4, 5, 8 and 10 are specifically addressed.

**Recommendation 1** states that biometric data should be regarded as a specific category of data. Special categories of data in Convention 108 are addressed in Article 6. Academic legal scholars and several reports tend to emphasize the importance of designating biometric data as sensitive data in European data protection legislation. Currently, biometric data are not yet considered sensitive personal data in Convention 108. As will be seen in Section 4 on the country responses, very few countries categorize biometric data as a special category of personal data. It is currently unclear what the precise consequences of such a categorization will be. Defining biometric data as sensitive personal data by default may result in imposing the very stringent requirements for the processing of such sensitive data for many basic applications. The Council of Europe should be aware of that.

**Recommendation 2** states that controllers of biometric systems should consider possible alternatives that are less intrusive for private life. The idea to employ less intrusive alternatives for biometric systems if reasonably possible can be linked to Article 5 of Convention 108. Some DPAs apply Recommendation 2, but unfortunately not all of them.

**Recommendation 4** notices the risk of function creep. This means that (biometric) data originally collected for one specific purpose is subsequently used for another purpose without the explicit consent of the data subject. This poses a significant risk to the data subjects' data protection rights. The development of new biometric technologies (so called second generation biometrics) may give rise to covert authentication of which data subjects are not aware. If data subjects are not aware of the collection of their biometric data, the controllers of the biometric system may process these data (also) for illegitimate purposes. The risk of function creep due to second generation biometrics is addressed in Section 5.

**Recommendation 5** states that biometric templates should be used instead of raw biometric data. This is a significant statement. Once raw biometric data is compromised, it cannot be used anymore as a method of authentication (subdivided into identification and verification) by the data subject. Once a biometric template is compromised, a new biometric template of the same original biometric feature (e.g. fingerprint) can relatively easy be generated. Section 6.2.4 discusses the method of biometric template protection in order to protect the data subject's biometric data. The country responses show that almost no data protection legislation and Data Protection Authority touches upon this possibility to strengthen the data protection framework for biometrics. It is very important to pay much more attention to this type of protection.

**Recommendation 8** states that the data subject should be informed about the purpose(s) of processing, the identity of the controller, the personal data that are processed, and the parties to which the data will be disclosed when this is necessary. These are important requirements for the controller of the biometric system, particularly with regard to current developments in biometric technologies. At present, covert authentication of data subjects is possible, which is a serious concern. Biometric characteristics of people can be captured from a distance and on the move, allowing the data subject's authentication without his consent. A data subject should know whether biometric characteristics are being collected and processed.

**Recommendation 10** addresses the need for technical and organisational measures to protect biometric 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. As mentioned above under 'recommendation 5' in this subsection, template protection can be a technical measure to tackle these potential risks. An elaborate overview of impostor threats and additional threats are discussed in Section 6.2, which includes the effective method of biometric

template protection (Section 6.2.4). In the next section we will discuss recent reports of and developments within the Council of Europe.

# 3 Recent developments within the Council of Europe

## 3.1 The Council of Europe's 2011 Parliamentary Assembly report

***General***

On 5 October 2006, the Parliamentary Assembly decided to refer to the Committee on Legal Affairs and Human Rights, for report, the motion for a recommendation on the need for a global consideration of human rights implications of biometrics.[8] The Committee, *de facto* acting as the Assembly's legal adviser, appointed Holger Haibach rapporteur. Mr Haibach's report was published in February 2011.[9] The report notes that the Committee has been increasingly concerned about the rapid and uncontrolled development of biometric technologies. In the opinion of the Committee, the European legal framework regarding the use of biometric data remains vague. The Parliamentary Assembly therefore strongly believes that the Council of Europe should take steps to ensure that this legal framework is enhanced and modernised.[10] The 2011 report contains recommendations to both the Council of Europe's Member States and the Committee of Ministers. These will be discussed in the next two paragraphs.

***Part 1 of the report: The Assembly's recommendations to Member States***

The 2011 report states that due to the events of 11 September 2001, security issues have become a major concern at the global level. They resulted in an ongoing search for secure and reliable methods of identification and verification of the intrinsic physiological characteristics of a human being through the use of biometrics. According to the report, the use of biometrics may offer a solution to various security concerns, but it also puts at stake several human rights. The Parliamentary Assembly is of the opinion that security has to be properly balanced against the protection of human rights. This balance is not yet appropriately reflected in Member States' legislation, according to the Assembly.[11] The Council of Europe Member States should therefore take further measures to improve the current European legal framework regarding biometrics. Rapporteur Mr Haibach advised

---

[8] Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Motion for a recommendation, Doc. 11066, available online at http://assembly.coe.int (search for Doc. 11066), Council of Europe 2006.

[9] Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Doc. 12522 (hereinafter Parliamentary Assembly Report 2011), available online at http://assembly.coe.int (search for Doc. 12522), Council of Europe 2011. The Assembly's recommendations to Member States are contained in its Resolution 1797 (2011), see Parliamentary Assembly, *The need for a global consideration of the human rights implications of biometrics*, Resolution 1797 (2011), available online at http://assembly.coe.int (search for Resolution 1797 (2011)), Council of Europe 2011.

[10] Parliamentary Assembly Report 2011, p. 3, §3.

[11] See Parliamentary Assembly Report 2011, p. 3, §1 and §2:

§1. "In the aftermath of the events of 11 September 2001, security issues have become a priority at the global level. They have led to an ongoing search for secure and reliable methods of identification and verification of the intrinsic aspects of a human being through the use of biometrics. The rapid development of biometric technology offers a possible solution to various security concerns, but it also puts at stake several human rights, such as the right to respect for private life, the right to a fair trial and the presumption of innocence, the freedom of movement and the prohibition of discrimination, as enshrined in the European Convention on Human Rights (ETS No. 5)."

§2. "The Parliamentary Assembly notes that there is a need to properly balance security and the protection of human rights and fundamental freedoms, including the right to privacy. The broad technical scope of biometrics, its rapid development and member states' willingness to make use of it for multiple purposes may not yet be appropriately reflected in member states' legislation in order to safeguard human rights. Once a new technology has found its way into everyday life, it becomes more difficult to implement or even adopt a proper legal framework. Member states should therefore deal with the legal issues relating to biometrics without delay."

the Member States to adopt specific legislation in this area and to produce a standardized definition of biometric data. Unfortunately, as will be seen in Section 7 on country responses, few countries have adopted specific legislation with regard to biometrics. The following suggestions of the Assembly for the Member States remain considerably relevant and important (**emphasis added**):

- adopt specific legislation on the use of biometric technologies to protect individuals from abuses of rights enshrined in the European Convention on Human Rights and other instruments on human rights protection, in particular to:
    - **elaborate a standardised definition of "biometric data"**;
    - revise the existing regulations concerning general protection of personal data by adjusting them to current applications of enhanced biometrical technologies;
- keep their legislation under review in order to meet the challenges stemming from the further development of biometric technologies, including so-called **"second generation" biometrics**;
- promote **proportionality** in dealing with biometric data, in particular by:
    - limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security clearly outweighs a possible interference with human rights and if the use of other, **less intrusive techniques** does not suffice;
    - providing individuals who are unable or unwilling to provide biometric data with **alternative methods of identification and verification**;
    - working with **template** data instead of raw biometric data, whenever possible;
    - enhancing **transparency** as a pre-condition for meaningful consent and, where appropriate, facilitating the **revocation of consent**;
    - allowing individuals **access** to their data, and/or the **right to have it erased**;
    - providing for appropriate storage systems, in particular by **reducing central storage** of data to the strict minimum;
    - ensuring that biometric data are only used for the **purpose** for which they have been lawfully collected, and preventing unauthorised transmission of, or access to, such data;
- establish, as appropriate, **supervisory bodies** to control the implementation of relevant legislation and provide for effective **remedies for individuals** in case of violations of their human rights and fundamental freedoms;
- strengthen the **compliance** of private sector applications of biometrics with existing data protection law, especially by:
    - ensuring **accountability** of data controllers;
    - promoting the **training** of relevant actors in the appropriate handling of personal data;
- promote **multidisciplinary research** on new biometric technologies that would ensure a balance between the need for enhanced security and the respect for privacy, human dignity and transparency;
- **assess potential risks** resulting from the use of biometrics for human rights and fundamental freedoms and exchange results between member states.

The 2011 report contains more recommendations than the 2005 report. The recommendations in the 2011 report are also made more concrete. The 2011 report highlights that Council of Europe Member States "[…] should adopt specific legislation in [the area of biometrics], produce a standardised definition of "biometric data", put in place supervisory bodies and promote multidisciplinary research."
The country reports (discussed in Section 7) demonstrate that currently very few countries have legislation specifically aimed at biometrics. Therefore, this recommendation of the 2011 report remains relevant.

Unlike the 2005 progress report, the 2011 report addresses the need of a **standardised definition** of biometric data. A short and proper definition of biometric data already mentioned in the introduction is: *'biometric data are measurable, physiological or behavioural characteristics that can be used to determine or verify identity'*.

The responses of 22 countries show that very few countries have adopted legislation specifically aimed at the protection of biometric data.[12] Georgia and Montenegro are the only two countries which have adopted a definition of biometric data. In **Georgia** biometric data is defined as "any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person". In **Montenegro** biometric data is defined as "data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly".

The 2011 report specifically addresses **second generation biometrics**.[13] In 2005, these biometrics were in the developing phase. The second generation includes biometric technologies enabling covert authentication through capturing biometric features from a distance and on the move, without the data subject's awareness and consent. This poses risks to the data subjects' data protection rights. None of the country reports addresses second generation biometrics.

The 2005 and 2011 reports both recommend alternative methods for biometric systems that are less intrusive for private life, although the 2011 report specifically addresses the need for **alternative methods of identification and verification** to be provided to individuals who are unable or unwilling to provide biometric data. The concept of subsidiarity is addressed in the country report of **Monaco**.[14] During an investigation conducted on 14 March 2011, staff of the Monegasque Data Protection Authority noted the existence of an unsecured central database for fingerprints for which no approval had been granted. The use of the biometric system had been stopped at the request of the Data Protection Authority.

The 2005 and 2011 report both recommend the use of **templates** instead of raw biometric data. The country reports show that very few countries address the need to use templates. Mr Haibach's recommendations regarding the use of templates have been noticed only in **Estonia** and **Italy**. The Estonian report underlines the importance to use biometric templates instead of raw biometric data.[15] The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects. For example, the storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases. Data protection legislation should include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.

The 2005 and 2011 report both address the need of provisions in data protection legislation containing the requirement that biometric data are only to be used for the **purpose** for which they have been lawfully collected. Due the development of second generation biometric technology enabling advanced capabilities of covert collection of biometric this requirement is even more important to prevent function creep. Unlike the 2011 report, the 2005 report includes the recommendation (Recommendation 1) to define biometric data as a **specific category of data**. This is a proper recommendation and underlines the vulnerability of biometric data. The country reports show that few countries have adopted legislation defining biometric data as a specific category of personal data. In **Estonia** biometric data is considered sensitive personal data.[16] In **Georgia** and **Macedonia** biometric data is considered a special category of personal data.[17]

### *Part 2 of the report: The Assembly's recommendations to the Committee of Ministers*

[12] See Section 7.2.1 for the analysis of country reports mentioning the adoption of legislation specifically aimed at biometric data.
[13] Section 5 elaborates on second generation biometrics.
[14] See Section 7.1.13 for the Monegasque response to the questionnaire.
[15] See Section 7.1.4 for the Estonian response to the questionnaire.
[16] See Section 7.1.4 for the Estonian response to the questionnaire.
[17] See Section 7.1.6 for the Georgian response to the questionnaire. See Section 7.1.11 for the Macedonian response to the questionnaire.

The 2011 report contains not only recommendations to the Council of Europe's Member States but recommendations to the Committee of Ministers as well.[18] The Parliamentary Assembly notes that the Council of Europe has already demonstrated its commitment to the protection of human rights in relation to data protection, particularly by adopting Convention 108 and through the work of its Consultative Committee.[19] The Assembly is of the opinion that "[t]he Council of Europe is therefore well placed to promote the adoption at the European level of rules on the use of biometrics".[20] The country reports (discussed in Section 7) demonstrate that currently very few countries have legislation specifically aimed at biometrics. Therefore, the following recommendations to the Committee of Ministers remain relevant and important (**emphasis added**):

- **revise the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** in order to adapt it to the challenges stemming from the development of new technologies, including biometric technologies, in particular by **developing a definition of "biometric data"**;
- prepare **guidelines** for member states on legislative frameworks that would strike a fair balance between the interests of the parties concerned, including those of security and privacy;
- **continue to observe the development of biometric technology** and its possible impact on the rights and freedoms enshrined in the European Convention on Human Rights and other Council of Europe instruments on human rights protection.

The country reports show that only 7 in 22 countries that responded to the questionnaire have adopted legislation and regulation specifically aimed at the protection of biometric data. These countries are (in alphabetical order) **Estonia**, **France**, **Georgia**, **Italy**, **Macedonia**, **Montenegro** and **Slovenia**.[21] France and Georgia are pioneering the field of data protection in general and biometric data in particular.[22] The processing of biometric data is regulated in French and Georgian DPL. France has strict regulation and since 2004 a doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. The Georgian data protection act contains several Articles regulating the processing of biometric data in particular.

In the opinion of the authors the 2011 Parliamentary Assembly's report captures all the main issues of the current legal debate on biometrics. The report contains many creative policy ideas regarding the regulation of biometrics. The central message is that additional regulatory measures, either soft law or hard law, are needed to be implemented in order to keep pace with developments in biometric technology and to harmonise the biometric legal framework across the CoE Member States. Data protection legislation should for example include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. The 2005 and 2011 report both recommend the use of templates instead of raw biometric data. Unfortunately, the country reports show that only Estonia and Italy have noticed and implemented this recommendation. Regulatory initiatives should also include a correct and useful definition of 'biometric data'. Section 7 on the country responses shows that very few countries have adopted legislation specifically aimed at the protection of biometric data. Georgia and Montenegro are the

[18] The Assembly's recommendations to the Committee of Ministers are also contained in its Recommendation 1960, see Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Recommendation 1960 (2011), (hereinafter Parliamentary Assembly Recommendation 2011), available online at http://assembly.coe.int (search for Recommendation 1960 (2011)), Council of Europe 2011.
[19] Parliamentary Assembly Report 2011, p. 5, §1.
[20] Parliamentary Assembly Report 2011, p. 5, §1.
[21] See Section 7.2.1.
[22] *Ibid.*

only two countries which have adopted a definition of biometric data. France and Georgia are pioneering the field of data protection in general and biometric data in particular.

## 3.2 The Consultative Committee's modernisation work of Convention 108

Currently, the Council of Europe's Consultative Committee is working on a modernisation of Convention 108.[23]. The Committee may make proposals for amendment of the Convention.[24] The Committee recently finalised the first stage of the modernisation work of the Convention, and proposed a new text.[25] This **modernisation proposal of Convention 108** was adopted in November 2012 by the 29th plenary meeting of the Committee. The new Article 6 on the processing of sensitive data **includes a provision concerning biometrics**.[26] It states that the processing of biometric data uniquely identifying a person shall only be allowed where the applicable law provides appropriate safeguards. These shall prevent the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. By means of this proposal the Committee categorizes biometric data as sensitive personal data, in order to particularly protect biometric data. However, it is not clear what the consequences of such a categorization are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that no longer a distinction can be made between more and less intrusive types of biometric processing. Moreover, in the Marper judgment, to be discussed in the next section, the European Court of Human Rights states that not all biometric data should be treated equally.

In its 2013 **draft explanatory report** the Consultative Committee states that it identified already in 2009 several angles of potential work on the convention, such as technological developments and information to be provided to the data subject.[27] As biometric technologies evolve quickly a major privacy concern of biometric recognition technologies is the advancing capability of capturing biometric features from a distance and on the move, which may allow for covert authentication. In such a case, the data subject is not aware of being identified by a biometric system, and probably did not give permission to collect biometric data, while a legitimate purpose for this collection may lack also. Convention 108 lacks criteria for the legitimate processing of data in general and the legitimate

[23] The Consultative Committee was set up by virtue of Article 18 of Convention 108.
[24] Convention 108, Article 19 in conjunction with Article 21.
[25] The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Modernisation of Convention 108* (hereinafter Modernisation Proposal 2012), Strasbourg: Council of Europe 2012, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf.
[26] The new Article 6 reads as follows:
1. The processing of genetic data, of personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where the applicable law provides appropriate safeguards, complementing those of the present Convention.
2. Appropriate safeguards shall prevent the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.
[27] Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD-BUR), *Draft explanatory report of the modernised version of Convention 108* (hereinafter Draft Explanatory Report 2013), Strasbourg: Council of Europe 2013, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR(2013)3_EN%20draft.pdf.

processing of biometric data in particular. One such criterion should be the explicitly given informed consent of the data subject.

The draft explanatory report categorizes **biometric data as sensitive data** if it enables the identification of an individual. Paragraph 54 of the Report reads as follows: "The processing of biometric data uniquely identifying a person (data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter) is also considered sensitive *per se*. This does not imply that all processing of 'biometric data' (such as pictures for instance) is to be considered as a sensitive processing but solely the processing which will enable the unique identification of an individual."
Paragraph 56 of the Explanatory Report mentions the importance to prevent potential risks (e.g. discrimination or injury to an individual's dignity or physical integrity) by means of employing "[…] appropriate safeguards (which are adapted to the risk at stake), such as the **data subject's consent**, a **risk analysis** or a statutory regulation of the intended process ensuring the confidentiality of the data processed".

The same remarks regarding the 2012 modernisation proposal apply to the 2013 draft explanatory report. Caution should be exercised when biometric data are considered sensitive personal data. It is not clear what the consequences of such a categorisation are. The importance of the data subject's consent and a risk analysis are evident, but second generation biometrics (Section 5) creates new legal challenges. New biometric technologies are capable of capturing biometric features from a distance and on the move, whilst the data subject is unaware. This poses significant risks for the individual's rights and freedoms.

In the 2012 **modernisation proposal** of Convention 108, drafted by the Council of Europe's Consultative Committee of Convention 108, the new Article 6 on the processing of sensitive data includes a provision concerning biometrics. By means of this proposal the Committee categorizes biometric data as sensitive personal data. The 2013 **draft explanatory report** of the Consultative Committee includes the same categorisation, although it is not clear what the consequences of such a categorization are. It may imply that no longer a distinction can be made between more and less intrusive types of biometric processing. In the Marper judgment, to be discussed in the next section, the European Court of Human Rights states that not all biometric data should be treated the same, because not all types of biometric data are equally intrusive. This strengthens the idea that research has to be conducted on the consequences of biometric data as a specific category of sensitive personal data prior to the introduction of a new article 6 in Convention 108.

## 3.3 The European Court of Human Rights: The Marper judgment

A crucial judgement in relation to the challenges of large-scale databases containing personal information was pronounced by the European Court of Human Rights on 4 December 2008, in the *S. and Marper* case[28]. The proceedings concerned two non-convicted individuals who wanted to have their records removed from the DNA database used for criminal identification in the United Kingdom.[29] More concretely, they asked for their fingerprints, cellular samples and DNA profiles, which had been obtained by police, to be destroyed.[30]

The Court held that there had been a violation of Article 8 as the retention of the fingerprints, cellular samples and DNA profiles of two persons who have been suspected, but not convicted of criminal offences is regarded a disproportionate interference with those persons' right

[28] *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgement of 4 December 2008 (hereinafter, *'Marper'*).
[29] As criminal proceedings against them had ended with an acquittal or had been discontinued (*Marper*, § 3).
[30] The applicants based their application on Articles 8 and 14 of the ECHR.

to respect for private life under Article 8 ECHR. The Court noted that "[…] all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention[31] as they relate to identified or identifiable individuals."[32] Although the Court recognized that fingerprints do not contain as much information as either cellular samples or DNA profiles, it stated that '[…] fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life […]'.[33]

In its ruling, the Court established that it is contrary to the requirements of Council of Europe's European Convention of Human Rights (ECHR)[34] to store for unlimited periods of time that type of personal information related to innocent people in a database of that nature.[35] It concluded that the blanket and indiscriminate nature of the powers granted to UK authorities constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered as necessary in a democratic society,[36] amounting therefore to a violation of Article 8 of the ECHR.[37] One of the major lessons to be learnt from the assessment of the European Court of Human Rights in the *Marper* case is that the storage of data such as fingerprints, cellular samples and DNA profiles in a database such as the one under examination is not inconsequential, irrelevant or neutral. On the contrary, the mere storage of such information conveys by itself a risk of stigmatisation:[38] *shadows of suspicion*, one could say, are projected upon those whose data is stored in a database dedicated to criminal identification and mainly destined to the storage of data of convicted people. Therefore, the storage of such data, when related to non-convicted individuals, has to be somehow limited.[39] If conveniently limited, it could be considered in accordance with the requirements of the ECHR.

But how should the applicable limits be determined? In the *Marper* judgement, the European Court of Human Rights underlined that the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and that they insist on the importance of foreseeing limited periods of storage.[40] Comparing such requirements with the blanket and indiscriminate nature of the power of retention granted in England and Wales, it judged this power to be a disproportionate interference with the applicants' right to respect for private life,

---

[31] Convention for the protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ETS No. 108 (Convention 108), entry into force 1 October 1985, Council of Europe.

[32] *Marper,* § 68.

[33] *Marper,* §78 and §84.

[34] Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November.

[35] As such storage represents an interference with the right to respect for private life established by Article 8 ECHR (*Marper*, § 77 and § 86) that cannot be judged proportionate.

[36] *Marper*, § 125.

[37] Art. 8 of the ECHR states: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[38] *Marper*, § 122. Moreover, the Court highlighted that the stigmatisation can be especially harmful when minors are concerned (ibid., § 124).

[39] The judgment reviews different national approaches in Europe to the taking and retention of DNA information in the context of criminal proceedings, and notes that the UK is the only Council of Europe Member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.

[40] *Marper*, § 107.

which cannot be regarded as necessary in a democratic society and thus is a violation of Article 8 of the ECHR.

Nevertheless, the idea that the duration of the retention of data needs to be proportionate to the 'purpose of collection' triggers, in situations like the one under examination, some problematic issues that were left unclear in the ruling. These problematic issues are linked to the fact that in databases such as the one in question the official grounds for collecting data are, as a matter of fact, not exactly the same as those pressing for as long as possible periods of storage of the data.

The Court also considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance between the retention of biometric data and the right to respect for private life.[41] In the opinion of the authors of this report it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a privacy impact assessment[42]. Such an obligation is provided in the proposed regulation, but it is not mentioned in the proposed directive.[43]

The European Court of Human Rights noted in its Marper judgment that "[…] all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of [Convention 108] as they relate to identified or identifiable individuals." Therefore, all biometric data allowing the identification of an individual is protected by Article 8 of the European Convention on Human Rights (ECHR), according to the Court.
The Court, however, recognized in its Marper judgment that fingerprints need to be distinguished from cellular samples and DNA profiles. The Court states that because of the information they contain, the retention of cellular samples and DNA profiles has a more important **impact on private life** than the retention of fingerprints. In the Court's judgment one can find an argument not to label all biometric data as sensitive personal data. It is not clear what the consequences of such a categorization are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that no longer a distinction can be made between more and less intrusive types of biometric processing. The Court also considers that States which claim to be a pioneer in the development of new technologies bear special responsibility for striking the right balance between biometric data retention and the right to respect for private life. In the opinion of the authors of this report it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a **privacy impact assessment**. Such an obligation is provided in the proposed regulation, but it is not mentioned in the proposed directive.

[41] *Marper*, § 112.
[42] A privacy impact assessment is sometimes termed otherwise, for example data protection impact assessment.
[43] Section 4.1 elaborates on the proposed regulation and proposed directive of the European Union.

# 4 Recent developments in the European Union

## 4.1 Proposals of the European Commission

On the 25th of January 2012, the European Commission published two significant proposals regarding the future European Union legal framework on data protection. The proposed EU Regulation[44] (hereinafter Proposed Regulation) involves the private and public sector, except for law enforcement, and the proposed EU Directive[45] (hereinafter Proposed Directive) involves law enforcement.

### *The Proposed Regulation*

It is remarkable that the term 'biometric' is only mentioned two times in the Proposed Regulation. It is stated in Article 4 containing a list of definitions and in Article 33 on data protection impact assessment:

**Definition of biometric data:** A definition of biometric data is proposed in Article 4(11) of the Proposed Regulation: "'biometric data' means any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data".

**Data protection impact assessment:** Article 33 of the Proposed Regulation comprises the requirement for the controller or processor of a biometric system to carry out a so-called data protection impact assessment, which is an assessment of the impact of the envisaged processing operations on the protection of personal data. This is required because the "[…] processing operations [of biometric data] in particular present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes […]".

**Biometric data not a special category:** Article 9 on the processing of special categories of personal data addresses genetic data and data concerning health as special categories of personal data which processing should be prohibited in principle (unless one of the exceptions in Article 9 is applicable), but biometric data is not mentioned as such a special category.

### *The Proposed Directive*

The Proposed Directive does not add much to the present legal framework with respect to biometrics. For example, it does not pay attention to the concept of privacy impact assessment (sometimes called data protection impact assessment). The term 'biometric' is only mentioned once in the Proposed Directive. It is stated in Article 3 containing a list of definitions:

**Definition of biometric data:** Article 3(11) of the Proposed Directive consists of the same proposed definition of biometric data as in the Proposed Regulation: "'biometric data' means any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data".

---

[44] Proposal for a Regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Proposed Regulation), COM(2012) 11 final, 2012/0011 (COD) C7-0025/12, available online at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0011_/com_com(2012)0011_en.pdf;

[45] Proposal for a Directive of the European parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereinafter Proposed Directive), COM(2012) 10 final, 2012/0010 (COD)C7-0024/12, available online at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0010_/com_com(2012)0010_en.pdf.

The Proposed Directive, unlike the Proposed Regulation, does not contain a requirement of a privacy impact assessment. Such a requirement is also lacking in the 2005 progress report and the 2011 Parliamentary Assembly report. Privacy impact assessments are important to limit the biometric systems' risks posed to the individual's rights and freedoms, particularly with regard to large biometric systems used for Eurodac, SIS, VIS and the European Biometric Passport, which are discussed in the next section.

It is noteworthy that the European Commission, unlike the Council of Europe, does not define biometric data as sensitive personal data or even a special category of personal data. The Council of Europe steers another course. In the modernisation proposal of the Consultative Committee regarding Convention 108 and the Consultative Committee's 2013 draft explanatory report of the modernized version of Convention 108 biometric data is considered sensitive data (see Section 3.2). The European Commission, like the Council of Europe's Consultative Committee, acknowledge the importance of a standardised definition of biometric data, as they both suggest one. The Committee's 2013 draft explanatory report contains the following definition of biometric data: "data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter". The European Commission and the Council of Europe are aware of the necessity to implement the requirement of a privacy impact assessment (sometimes called a data protection impact assessment). The Proposed Regulation contains such a requirement in Article 33, and the 2012 Modernisation Proposal of the Council of Europe's Consultative Committee includes such a requirement in Article 8bis(2). The country reports show that no Member State has yet implemented in their data protection legislation an obligation to perform a privacy impact assessment. However, France, Italy, Macedonia, Monaco, Montenegro and Slovenia incorporated the requirement of prior checking in their data protection legislation.

## 4.2 European Union's Eurodac/SIS/VIS/European biometric passport

### 4.2.1 Eurodac

The Eurodac system, operational since 15 January 2003, enables European Union (EU) countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union. By comparing fingerprints, EU countries can determine whether an asylum applicant or a foreign national found illegally present within an EU country has previously claimed asylum in another EU country or whether an asylum applicant entered the Union territory unlawfully. The Eurodac system consists of: a central unit managed by the European Commission, a central computerised database of digital fingerprints, electronic means for data transfers between Member States and the central database. The 2006 Commission Staff Working Document[46] of the Commission of the European Communities shows that in 2005 the EURODAC Central unit has again given very satisfactory results in terms of speed, output, security and cost-effectiveness.

Only national authorities responsible for asylum applications have access to the central database. These are the three categories of persons for whom Eurodac gathers information: asylum seekers older than 14 years, aliens apprehended in connection with the irregular crossing of an external border and aliens illegally on the territory of a Member State. The following data are registered: the Member State of origin, the digital fingerprint, the sex and the reference number used by the Member State of origin. When there is an alert the data are transferred through the DubliNet

[46] Commission of the European Communities, *Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit,* Commission Staff Working Document, SEC(2006) 1170, Commission of the European Communities 2006, available online at http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/sec_2006_1170_en_en.pdf.

system. DubliNet is a secure electronic communication network between the national authorities dealing with asylum applications. The two involved Member States can exchange personal data through DubliNet that differ from Eurodac data, like name, date of birth, nationality, photo, details on family members and in some cases addresses.
Data subjects entered on the Eurodac database do not carry a document containing the biometric(s) for verification or identification because the databank is the human body itself. Every time the person is subject to a control for the purposes of Eurodac, they will have to provide a body reading which can then be checked against the data held in the database. The arrangements have attracted considerable criticism because Eurodac requires the mandatory disclosure of biometric information by people who have not committed a crime. Some commentators have questioned whether it is morally justifiable to require asylum seekers and aliens to provide biometric data which is then placed in a public arena and out of their immediate control. The increase in recent years of the so-called 'special searches' triggered concerns about possible misuse of the purpose of this functionality by national administrations.[47] Therefore, the Commission has included in its proposal for the amendment of the Eurodac Regulation a requirement for Member States to send a copy of the data subject's request for access to the competent national supervisory authority.[48]

The Eurodac system, operational since 15 January 2003, enables European Union (EU) countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union. The Eurodac system has attracted considerable criticism because it requires the **mandatory disclosure of biometric information** by people who have not committed a crime. The following data are registered: the Member State of origin, the digital fingerprint, the sex and the reference number used by the Member State of origin. The registration of biometric data and other additional information of the data subject may pose risks such as **function creep**, particularly because the disclosure of biometric data is mandatory.

### 4.2.2 The Schengen Information System

The Schengen Information System is the largest information system for public security in Europe, which has been operational since 1995. The Schengen Information System (SIS) was established as an intergovernmental initiative under the Schengen Convention, now integrated into the EU framework. It is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. It holds information on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents, that may have been stolen, misappropriated or lost. Information is entered into the SIS by national authorities and forwarded via the Central System to all Schengen States.
Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system.
It will be one of the world's largest IT systems in the field. It will consist of three components: a Central System, EU States' national systems and a communication infrastructure (network) between the Central and the national systems. The European Commission is currently managing the development of the SIS II Central System, while SIS II national systems are being developed by the

[47] European Commission, *Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit* 2011 (Report from the Commission to the European Parliament and the Council), COM(2012) 533 final, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0533:FIN:EN:PDF.
[48] *Ibid.*, section 1.5.

Schengen States. SIS II introduces the ability to process biometric data, particularly fingerprints and face scans. All 27 EU Member States, plus Iceland, Norway, Switzerland and Lichtenstein will be connected to SIS II. A European Parliament report has pointed out that there has been no targeted impact assessment on the use of biometrics, and that specific provisions detailing fall back procedures to protect individuals who are wrongly identified are lacking. The real capabilities of the biometric identifiers chosen within SIS II for identification have not yet been assessed.
So far, a record in the SIS did not include more than 2 lines worth of data, in other words, not more than the simple search entry. SIS 2 will thoroughly change this. From now on, photos, fingerprints and, if necessary, even DNA profiles will be included in the SIS personal records. The character of the system is therefore substantially changed. Up to now, SIS has been used first and foremost by officers controlling entry at the borders. In future, it will increasingly be police crime investigation units who are interested in the SIS.
Competent authorities will use SIS II to exchange data, including biometric fingerprints and face scans, using the same platform as VIS but with a separate access route. Levels of access will vary and will be regulated in accordance with European data protection provisions. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities. The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. The possible use of SIS II biometric data for investigative purposes might pose serious risks for data subjects if the significance of biometric evidence is over-estimated by the courts. The use of biometrics for identification (comparison of one to many) is proposed for future implementation within the SIS II system.

The Schengen Information System (SIS) is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics (e.g. photos, fingerprints and, if necessary, even DNA profiles), the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. As soon as SIS II becomes operational it will increasingly be police crime investigation units who are interested in the SIS. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities. The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. The use of (biometric) data for another purpose than originally collected for, which is called **function creep**, poses serious risks for the individual's rights and freedoms, particularly if more authorities will be granted access to SIS.

### 4.2.3 The Visa Information System (VIS)

The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. It enables the exchange of visa data in relation to Schengen uniform visas and "national visas" among the Member States that have abolished checks at their internal borders. Its objectives is to facilitate the fight against fraud, to contribute to the prevention of "visa shopping", to improve visa consultation, to facilitate identifications for the application of the Dublin II regulation and return procedures, to improve the administration of the common visa policy and to contribute towards internal security and combating terrorism. To this end, the VIS database will include information about personal identification of visa applicants (incl. biometrical data), status of visa, authority that issued the visa, and record of persons liable to pay board and lodging costs.
The VIS is expected to handle more than 20 million visa requests from 25 participating states and 45 million requests to check on the validity of issued visas per year. The list of countries whose nationals

must comply with the Schengen visa requirement in order to cross the external frontiers is set by Council Regulation (EC) 539/2001 of 15 March 2001.
Biometric data (digital facial image and fingerprints) have been added to the VIS. The Council Guidelines of 13 June 2002 indicate "digitized photographs and other biometric data on the holder of the visa could also be entered in VIS when they are added to the visa file".

The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. The VIS database will include information about personal identification of visa applicants (including biometrical data such as facial image and fingerprints), status of visa, authority that issued the visa, and record of persons liable to pay board and lodging costs. Because the disclosure of biometric data and other additional information is mandatory its registration may pose risks such as **function creep**.

### 4.2.4 The European Biometric Passport

The European Commission adopted a proposal for a Regulation on standards for security features and one biometric in EU citizens' passports in 2004.[49] In the Explanatory Memorandum to the Commission Proposal, the Commission recalled that the idea of a "European Passport" was already accepted by the Member States "to facilitate the free movement of nationals of Member States" and as an instrument "to promote any measures which might strengthen the feeling among nationals of the Member State that they belong to the same Community".[50] Following the events of 11/9 the need was felt to enhance the security of travel documents by adding biometric elements.[51] The main reason for preferring a regulation to a directive is that the proposal provides for a total harmonization of a minimum standard for the security elements of such documents, and their biometric identifiers, thus leaving no room for discretion to the Member States.[52] In the Explanatory Memorandum, the creation of a 'European register for issued passports' is called a second step, but the Commission stresses that further research is necessary to "examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection".[53]

The proposal was in line with the ICAO report that adopted a facial recognition standard based on a contact-less chip in May 2003. ICAO recommended the use of a single biometric technology by all States, as this would ensure global interoperability, but allowed States to use two biometrics.[54] The Council added a second mandatory biometric identifier to the proposal.
The European Parliament's non-binding legislative resolution on the Commission proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports from 2 December 2004[55] was adopted by 471 votes in favour to 118 against and 6 abstentions.[56] The

[49] Commission of the European Communities, 'Proposal for a Council Decision on standards for security features and biometrics in EU citizen's passports', Brussels, 18 February 2004, COM(2004) 116 final, 20p.
[50] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 2.
[51] Ibid.
[52] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 6.
[53] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 8.
[54] International Civil Aviation Organisation (ICAO) in Document 9303, See ICAO, Biometrics Deployment of Machine Readable Travel Documents, ICAO TAG MRTD/NTWG Technical Report: "Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using MRTDs " (Montreal ICAO, 2003).
[55] European Parliament's report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), including voting list and all amendments, via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2004-0028+0+DOC+PDF+V0//EN.
[56] Article 29 Data Protection Working Party's Opinion (WP 112) on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel

resolution declares that the biometric features in passports shall only be used for verification of the authenticity of the document and the identity of the passport holder and that it shall be stored on "a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored". Moreover, the Parliament introduces an amendment to the draft Regulation text specifically stipulating that "no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up". According to the report on the Committee on Civil Liberties, Justice and Home Affairs of 25 October 2004, "the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets." The Council adopted Regulation (EC) No 2252/2004 on 13 December 2004, but did not take account of the suggestions and requests of change laid down by the Parliament.[57]

On 26 November 2004 the European Parliament adopted the proposal thus amended but introduced a large number of limitations. The Members of Parliament voted to clearly limit the kinds of information to be stored on the passports; they voted against the storage of the data in a central database and in favor of giving Data Protection Authorities oversight over the whole process. The Council of European Justice and Home Affairs ministers did not adopt any of the amendments of the Parliament. In December 2004, the Council adopted the regulation. The choice for mandatory facial images as well as finger scans and the idea of a centralized database was not questioned.[58]

Article 1 of the Regulation contains the main idea: passports and travel documents shall include a storage medium, which shall contain a facial image. Member States shall also include fingerprints in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

On all pages inside the passport or travel document a unique document number should be printed or perforated or, in passport cards, a unique document number should be integrated using the same technique as for the biographical data. It is recommended that in passport cards the unique document number is visible on both sides of the card.[59] The Regulation does not give any information about the possibility of establishing a European centralized database and leaves the decision whether or not to create a national database to the national governments.

Persons to whom a passport or travel document is issued shall have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure.[60]

No information in machine-readable form shall be included in a passport or travel document unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport or travel document by the issuing Member State in accordance with its national legislation.[61]

The biometric features in passports and travel documents shall only be used for verifying: (a) the authenticity of the document; (b) the identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law.[62]

---

documents issued by Member States, *Official Journal L 385, 29/12/2004 p. 1-6*, adopted on 30 September 2005.

[57] *Ibid.*, p. 5.

[58] Council Regulation of 10 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Doc. 15152/04, 9p. and one Annex, 5p.

[59] Council Regulation of 10 December 2004, Annex, sub 3C.

[60] Council Regulation of 10 December 2004, Article 4, 1°.

[61] Council Regulation of 10 December 2004, Article 4, 2°.

[62] Council Regulation of 10 December 2004, Article 4, 3°.

All in all little attention has been paid by the EU legislator to the requirement of proportionality and necessity.[63] A proportionality argument can be found in the assertion that the "harmonisation of document formats and of their security features will provide a guarantee against counterfeiting. By preventing forgery and counterfeiting of travel documents the Commission intends to enhance the high level of security, a target set out both by the Treaty and the European Council of Thessaloniki".[64] However, nowhere in the Proposal or in the Council Regulation is it demonstrated that two biometrics and a centralized database are proportional and necessary in a democratic society. The sheer fact that the Commission had limited itself to making only one biometric obligatory and seemed hesitant to argue for and propose databases at national or European level, indicates that it had taken another view. On the basis of current data protection legislation choices for more biometrics and for a centralised database do not seem automatically justified.

The Council of European Justice and Home Affairs ministers adopted Regulation (EC) No 2252/2004 ('Regulation on standards for security features and biometrics in passports and travel documents issued by Member States') on 13 December 2004 without taking into account proposed amendments of the European Parliament. The choice for mandatory facial images as well as finger scans and the idea of a centralized database was not questioned. Furthermore, little attention has been paid by the EU institutions to publicly account for meeting the requirements of proportionality and necessity. It can be concluded that the EU does not always pay adequate attention to privacy issues regarding biometrics. The country reports show that very few countries incorporate privacy protecting provisions in legislation concerning biometrics.

[63] In its February 2004 Proposal, the Commission inserts a full paragraph on 'subsidiarity and proportionality', but a closer look reveals that these requirements are only understood in their federalist meaning, viz. to explain why this issue is taken up by the Union and not left to the discretion of the Member States.
[64] *Ibid.*

# 5 Second generation biometrics

## 5.1 What are second generation biometrics?

The 2011 report of the Parliamentary Assembly recommends the Council of Europe's Member States to keep their legislation under review in order to meet the challenges stemming from the further development of biometric technologies, including the so-called 'second generation' biometrics. Second generation biometrics aims to identify a person on the basis of his or her actual behaviour or activities.

The handling of first generation biometric data (e.g. fingerprints and iris scans) already creates fundamental discussions about the scope of data protection and human rights law. The introduction of soft biometrics, i.e. the use of general traits such as gender, weight, height, age, or ethnicity for automated classification, is even more contested. It has attracted criticism of indiscriminate social sorting, as automated decisions are created that divide people into categories for further processing. What are the legal implications of automated sorting of people on the basis of their behaviour (and/or general traits) into classifications such as for example, Asians and non-Asians, young and old, gay and hetero, and so forth? On the one hand, as machines are taking the decisions, the act of sorting takes on a seemingly neutral dimension. On the other hand, the embedded systems, ambient intelligence, distant sensing and passive biometrics involved require no conscious cooperation from subjects and thus pose a challenge to the traditional concepts used in the fields of data protection and human rights.

What are the important elements of second generation biometrics and will they give rise to a new set of legal issues to be analysed and discussed? We identify two developments in biometrics that together form the main step away from the first generation applications of the technology. The first is the emergence of new biometric traits and the second is the shift to embedded biometric systems, with elements such as distant sensing and 'passive' biometrics. These distinct developments are the basic changes that might catapult us into the world of ambient intelligence and ubiquitous computing. Then, the already complex legal assessment of biometric data handling will be taken to a different level altogether and pose serious challenges to existing legal approaches (basically based on data protection law). The dream of second generation of biometrics is a person's identification on the basis of that person's dynamic behaviour. In fact, the attempt is not made to identify a person, no: the objective is to read the person's mind.

The 2011 report of the Parliamentary Assembly recommends the Council of Europe's Member States to keep their legislation under review in order to meet the challenges stemming from the further development of biometric technologies, including the so-called 'second generation' biometrics. Second generation biometrics aims to identify a person on the basis of his or her actual behaviour or activities. Second generation biometrics comprises a new type of biometric features such as gait (manner of walking), voice, body odour, ECG (brainwave pattern), EEG (electrical activity of the heart), body temperature, and pupil dilation. These biometric characteristics can sometimes be collected from a distance whilst the data subject is unaware. This makes it more difficult to monitor whether biometric controllers comply with data protection legislation (e.g. informed consent by the data subject prior to biometric data processing).

## 5.2 Concerns about second generation biometrics

Problematic legal aspects of second generation are covert data capture, lack of transparency and consent. Many second generation biometrics are collected whilst the data subject is unaware. Data is collected from a distance and the collection does not need to be apparent. The paradigm change here is that tracking and tracing becomes the norm resulting in a surveillance society. Instead of enrolling and identifying or verifying a person, second generation biometrics is aimed at a categorisation of individuals. The threats caused by this de-personalisation are many fold. Of course unjustified selection according to profile will result in discrimination. Stigmatisation will occur and

will involve allocation to a group on the basis of relatively random profiles which will impact the persons' future. Confrontation of individuals with unwanted information is another side effect that is very likely to occur. Finally, there will be unknown effects in linking dispersed information.

One of the most fundamental challenges in the protection of personal biometric data is related to the incremental change from visible to invisible data collection. The obvious risk that the systems (and not only personal data) may be used by other persons and for other purposes than foreseen (**function creep**) is difficult to minimize, without the traditional possibilities for individual participation (informed consent). A number of transparency tools can be developed that give the individual more insight into who is taking which decisions on the basis of data collected. The current lack of possibilities to enforce individual participation is regrettable when it comes to assessing the applicability of data protection law in situations where the subject is unaware of the invisible data collection. Therefore, the main legal concern regarding second generation biometrics is the applicability of data protection regulation in those situations and the specific use of the data for **profiling**. Firstly, there is the applicability of data protection regulation. If no attempt is made to identify a person, can we define the data concerned as personal data? If not, what guarantees remain against unwarranted and unfit social categorisation? Secondly, there is the issue of profiling. It is not clear whether and when profiling falls directly under the Convention. In conclusion, the use of second generation biometrics will have to lead to a re-assessment of the traditional data protection approach that only data relating to identified or identifiable persons have to be protected.

The Council of Europe's 2010 Recommendation on profiling[65] is an important document for Member States. It contains recommendations to the collection and processing of personal data used in the context of profiling notably by taking measures to ensure that the principles set out in the appendix to this Recommendation are reflected in their law and practice. The Recommendation states that collected data (e.g. traffic data, consumer buying habits, geo-location data, data stemming from social networks, video surveillance systems, biometric systems and RFID systems) are processed by "[…] calculation, comparison and statistical correlation software, with the aim of producing profiles that could be used in many ways for different purposes and uses by matching the data of several individuals", while "[…] the development of ICTs enables these operations to be performed at a relatively low cost". Due to this linking of a huge amount of individual, anonymous observations the profiling technique is capable of having severe impact on the people concerned by placing them in predetermined categories, frequently without their knowledge. Data subjects' profiles make it possible to generate new personal data – even sensitive data – for which no consent has been given by the data subject. The Council of Europe concludes in its 2010 Recommendation that it is necessary to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Several recommendations are provided in the annex.

Due to second generation biometrics an incremental change from visible to invisible data collection may occur. Biometric data may be originally collected for one specific purpose, but subsequently used for another purpose (**function creep**). It becomes more difficult to exercise the right to object to certain types of data processing. Moreover, biometric data may be used for **profiling** activities, while it is not clear whether and when profiling falls directly under the Convention. The Council of Europe concludes in its 2010 Recommendation that it is necessary to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Second generation biometrics can be used for profiling, meaning that individuals can be categorized. Unjustified selection due to profiling may result in **discrimination** and **stigmatisation**.

[65] Council of Europe Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).

# 6 Intrinsic errors of and impostor threats to biometric systems

## 6.1 Intrinsic errors of biometric systems

All biometric systems (without exception) have some intrinsic errors having a negative effect on the system's performance and accuracy (i.e. efficacy). The main errors are the failure to enroll, failure to acquire, false accept error and false reject error, usually expressed in the accompanying rates (i.e. proportion or probability).

The **failure to enroll rate (FTE)** reflects the proportion of individuals of whom the biometric system is unable to extract sufficient characteristics, e.g. because the individual is unable to produce an image of sufficient quality, is unable to reproduce his biometric consistently, or is unable to present the required biometric, as he for example misses a particular finger. This error is an important consideration since enrolment failures directly reduce the efficiency, accuracy and usability of the biometric system.

The **failure to acquire rate (FTA)** reflects the proportion of attempts for which the biometric system is unable to capture an image of sufficient quality, e.g. due to an injured finger. Although the FTE and FTA are usually quite low, it is necessary to have a fall back procedure in case such failures occur, e.g. human intervention, enrolment of another finger or enrolment of a different modality (i.e. the kind of biometric) provided that the system comprises of at least two different biometric modalities, for example iris recognition and fingerprint recognition.

The **false acceptance rate (FAR)** is the probability a biometric system will incorrectly accept someone. This could be an illegitimate user who accessed the biometric system by means of spoofing, but also a person whose image/template is by accident mistakenly matched with another enrolled person's image/template. FAR is considered to be the most crucial security error of a biometric system and generally ranges from 1% (low security applications) to 0.00001% (very high security applications), although biometric vendors often quote unreliable FAR numbers and provide a best case scenario. These rates normally concern passive impostor attempts (an imposter's attempt to spoof the system is observed by staff) as the actual rates of a biometric system in operation often remain unnoticed. The actual FAR is probably much higher, because tracing back in case of a false acceptance will generally reveal the person who actually belongs to the biometric instead of revealing the impostor. Low false accept errors are particularly required in high security applications (e.g. nuclear power plants).

The **false rejection rate (FRR)** is the probability a biometric system will incorrectly reject someone. Generally, FRR ranges from 0.1% to 20%[66], although an FRR of 0.1% is not likely in practice. A 2005 study conducted in the UK by Atos Origin resulted in an FRR of approximately 20% for fingerprints.[67] False rejection errors are inconvenient to a legitimate user, who needs to re-attempt the authentication process or has to be authorised by means of an alternative method (e.g. a different biometric modality or human intervention).[68]

It has to be noted that FRR and FAR are not performance criteria.[69] These numbers are units to measure the performance. The criteria are determined by the biometric system operator (also termed processor) by setting the threshold. The FAR and FRR are inversely proportional, i.e. decreasing the FAR will result in an increased FRR and vice versa. This phenomenon is sometimes called the trade-off between FAR and FRR. Main consequence is that reducing the FAR (in order to

---

[66] European Commission Joint Research Centre, Institute for Prospective Technology Studies, *Biometrics at the Frontiers: Assessing the Impact on Society* (hereinafter European Commission 2005), Seville, 2005, p. 163. Available online at: http://www.biteproject.org/documents/EU_Biometrics_at_the_Frontiers.pdf.

[67] See http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf.

[68] Irish Council for Bioethics Opinion 2009, p. 8.

[69] Wetenschappelijke Raad voor het Regeringsbeleid (WRR), the Dutch Scientific Council for Government Policy, Webpublicatie nr. 51, *Het biometrisch paspoort in Nederland. Crash of zachte landing* (hereinafter WRR 2010), Max Snijder, 2010, p. 111-112. Available online at http://www.wrr.nl/.

attain a higher security level), results in an increased FRR (implying reduced convenience and efficiency), and vice versa. The FAR and FRR can be adjusted by the system operator. In has to be noted that false acceptance errors and false rejection errors (and all other errors involving biometric systems) are usually tested in laboratory environments, and consequently may not be an accurate indication of the system performance in practice. Biometric system vendors often refer to testing results of the NIST (National Institute of Standards and Technology), which is the most authoritative testing institute regarding biometrics. The NIST, however, does not take into consideration particular operational circumstances, which evidently affect the testing results of a biometric system.[70] Therefore, every biometric system, especially large-scale systems, needs to be tested in a 'real world' situation.

The point of intersection of FAR and FRR (i.e. FAR=FRR) is called the equal error rate (EER), which is considered to be the best choice of operation for civilian applications.[71]

All four intrinsic errors negatively affect the efficacy and efficiency of a biometric system. The FTE can often be reduced by means of assistance of trained personnel (human intervention) to the individuals who need to provide their biometric. The FAR and FRR negatively affect the accuracy and efficiency of the entire biometric system and mainly depend on the quality of the biometric images (e.g. fingerprint or facial image). Therefore, the FAR and FRR can be reduced (although not to zero)[72] by increasing the quality of biometric images.[73] The quality of images is crucial particularly in large-scale systems (systems that have stored millions of templates (i.e. transformed images/scans)) running in identification mode (1:n). Identification based systems, namely, by definition require a centralized database in which possibly millions of stored biometric templates are to be compared with the query biometric template (i.e. the fresh template as opposed to the stored reference template). The more images or templates available to compare with the query template, the higher the negative influence of image/template quality and the higher the errors involved (e.g. FAR, FRR) will be.[74] For that reason, a switch from verification based biometric systems to identification based systems inherently comes along with increased error rates. Therefore, reducing error rates is even more important in identification based biometric systems. The FTA furthermore (but also the FTE, FAR and FRR) can be reduced by employing multimodal biometric systems, which make use of several biometric modalities. Two design modes offer best accuracy: (1) multiple biometrics from the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger).[75]

Aware of the need for quality control, the National Institute of Standards and Technology (NIST) in 2004 introduced the NIST Fingerprint Image Quality (NFIQ) algorithm, which facilitates the

---

[70] WRR 2010, p. 31.

[71] European Commission 2005, p. 49.

[72] This is due to the *intra-class variation*. The matching process (between biometric sample and stored reference template, provided that the biometric feature is stored by means of a generated template instead of the raw biometric data) does not provide a 100 per cent accurate binary yes/no answer regarding the fact whether the sample and stored reference template are identical. Instead, it is a statistical process since no two biometric samples (of the same biometric modality) from the same person are ever completely identical and therefore the biometric systems, by their very nature, generate results that are 'probabilistic'. This phenomenon is called intra-class variation and is caused by several factors such as varying ambient conditions (e.g. atmospheric humidity), imperfect imaging of the biometric, (slightly) changed biometric characteristics, or changes in the interaction between user and sensor. Due to this variation every time a person presents his biometric, the systems' algorithm provides a score of the degree of similarity between the sample and the stored reference template. The higher the degree of similarity, the more "certain" the conclusion that the two templates belong to the same individual. The threshold level can be adjusted, depending on the specific application of the biometric system. This intra-class variation produces the intrinsic errors FAR and FRR.

[73] Unfortunately, international quality standards with respect to biometric images/templates are lacking.

[74] WRR 2010, p. 143.

[75] Irish Council for Bioethics Opinion 2009, p. 55.

measurement of image quality of fingerprints in order to reduce the FAR and FRR.[76] The NFIQ is currently the most important instrument to assess the quality of fingerprints, yet not sufficiently to guarantee uniform quality.[77] Development of international quality standards for various biometric characteristics is ongoing, but not yet available in the coming years.[78]

All biometric systems (without exception) have some intrinsic errors having a negative effect on the system's performance and accuracy (i.e. efficacy). The main error rates are the failure to enrol (FTE), failure to acquire (FTA), false accept error (FAR) and false reject error (FRR). Although the FTE and FTA are usually quite low, it is necessary to have a fall back procedure in case such failures occur, e.g. human intervention, enrolment of another finger or enrolment of a different modality (i.e. the kind of biometric) provided that the system comprises of at least two different biometric modalities, for example iris recognition and fingerprint recognition. FAR is considered to be the most crucial security error of a biometric system and generally ranges from 1% (low security applications) to 0.00001% (very high security applications), although biometric vendors often quote unreliable FAR numbers and provide a best case scenario. The actual FAR is probably much higher. The FAR and FRR can be adjusted by the system operator. The FAR and FRR are inversely proportional, i.e. decreasing the FAR will result in an increased FRR and vice versa. The main consequence is that reducing the FAR (in order to attain a higher security level), results in an increased FRR (implying reduced convenience and efficiency), and vice versa. All four intrinsic errors negatively affect the efficacy and efficiency of a biometric system. The FTE can often be reduced by means of assistance of trained personnel (human intervention) to the individuals who need to provide their biometric. The FAR and FRR can be reduced (although not to zero) by increasing the quality of biometric images. The FTA furthermore (but also the FTE, FAR and FRR) can be reduced by employing multimodal biometric systems, which make use of several biometric modalities. Two design modes offer best accuracy: (1) multiple biometrics from the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger). It can be concluded that the biometric systems' performance and accuracy depend on error rates, which can for example be reduced by human intervention, multimodal biometric systems and higher quality of biometric images. The European legal framework on data protection should include provisions aiming to reduce the errors of biometric systems, such as provisions on human intervention, multimodal biometrics, high quality images and fall-back procedures.

## 6.2 Risk analysis of biometric systems

### 6.2.1 Introduction

A biometric system may encounter problems. Biometric data, namely, is not only valuable to the controller of the biometric system, but can also be valuable to impostors as they may use such data to commit, for example, identity fraud. In order to acquire these data they may attack a biometric system. Additionally, it is not implausible that third parties obtain biometric data through intentional or unintentional data leakage. Several risks, which are not listed exhaustively, are discussed in the next sections. Firstly, a few categories of intentional impostor threats are addressed (section 6.2.2) as these are often the most striking threats to a biometric system. However, threats do not merely arise from impostor attacks, but may also emerge due to intentional or unintentional acts of the system's controllers, personnel or other individuals having legitimate access to biometric systems and/or data. Therefore, secondly, examples of additional threats are provided (section 6.2.3), which will place the striking impostor attacks in another perspective. Section 6.2.4 at last, addresses methods to

[76] WRR 2010, p. 24.
[77] *Ibid*., p. 36.
[78] *Ibid*.

overcome the problem of compromised biometric templates as it is a major concern in biometric applications.

### 6.2.2 Impostor threats

Impostor threats can be defined as the impostors' intentional efforts to illegitimately access or circumvent the biometric system. A significant impostor threat is an attack to the biometric database (*database attack*). Large-scale central databases are more susceptible to such database attacks, compared to decentralized databases. Although large-scale databases are often better protected, an impostor can obtain a large amount of (valuable) biometric information through one attack. Impostors may also take away objects with latent fingerprints on it.

Jain *et al* have categorized impostor threats into three main classes, with regard to the biometric system (not necessarily including a biometric database): administration attack, nonsecure infrastructure, and biometric overtness.[79]

***Administration attack*** concerns vulnerabilities due to improper administration of a biometric system and comprises the integrity of the enrollment process (e.g. whether the correct credentials are presented), and coercion or collusion between an impostor and the system operator (e.g. intentional leakage) or a legitimate user (e.g. enrollment fraud).

***Nonsecure infrastructure*** concerns vulnerabilities due to manipulation of software, hardware and communication channels inside the biometric system, possibly resulting in security breaches. Examples of infrastructure vulnerabilities are: *Trojan horse attacks* (input of malicious software to manipulate data in the biometric system), *replay attacks* (circumventing the sensor by inserting a recorded image from a legitimate user back into the biometric system), *tampering* (modifying data in stored templates or during authentication in order to guarantee a high match score of his own biometric), *masquerade attack* (submitting an artifact image, created from a fingerprint template, but not necessarily resembling the original image, to ensure a match), *substitution attack* (accessing or overwriting a stored template, or replacing this template by the impostor's template), *overriding the yes/no response* (inserting a false yes (i.e. match) response in the biometric system in order to pose as a legitimate user).[80]

***Biometric overtness*** concerns vulnerabilities due to the use of physical artifacts of a biometric trait subsequent to the covert acquisition of such traits from a genuine user. If the biometric system is incapable of distinguishing between a genuine biometric presentation and an artificial biometric spoof, an impostor can circumvent the system by means of spoofing.

### 6.2.3 Additional threats

Several other threats apart from impostor threats exist, although this section does not intend to give an exhaustive overview of all possible additional threats. The examples given merely show that threats to biometric data and systems not only arise from impostor attacks, but also from acts of controllers of biometric systems, personnel or other individuals having legitimate access to biometric systems and/or data, which acts may be performed intentionally. Biometric information, namely, may be originally collected for one specific purpose, but subsequently intentionally used for another purpose. This phenomenon is generally termed **function creep**. Other examples of threats are **surveillance** activities (**tracking** and **tracing** of individuals) or otherwise excessive control activities by governmental institutions or private companies, as biometric data can be covertly collected. Also the **linking** of biometric data to other personal information, a threat which is particularly present in case of storage of biometric data in databases, may cause privacy concerns. Biometric templates stored in such databases may also be matched against templates in other databases, a phenomenon called **cross-matching**. Unintentional threats, on the other hand, are threats to the biometric system or

---

[79] Jain, A.K., Nandakumar, K., and Nagar, A., *Biometric Template Security* (hereinafter Jain *et al* 2008), EURASIP Journal on Advances in Signal Processing, Special Issue Advanced Signal Processing and Pattern Recognition Methods for Biometrics Volume 8, Article ID 579416, 2008, available online at http://www.hindawi.com/journals/asp/2008/579416, p. 2-3.

[80] Irish Council for Bioethics Opinion 2009, p. 10; Jain *et al* 2008, p. 4.

biometric data without necessarily the incidence of deliberate misuse. Some examples of unintentional threats are **system failures**, accidental **leakage** (by individuals who have access to the biometric data), **derivation of additional personal information** from biometric data (e.g. ethnic origin or health information) or the case where some **biometric data are (left) in the public domain** (e.g. someone's face as it is 'public information' or fingerprints left on a glass).

### 6.2.4 Biometric template protection

***General***

Several mechanisms to overcome the vulnerabilities addressed in the preceding sections are human intervention, human supervision, liveness detection and multimodal biometrics. A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric.[81] Moreover, in comparison with conventional security methods (e.g. using a password or PIN), biometric characteristics are not revocable and cannot be reissued. Therefore, academic research is mainly focused on the protection of biometric templates.
A major challenge in developing a secure biometric template is to handle the intra-class variation[82]. As a result of this intra-class variation, it is impossible to store a biometric template in an encrypted form (through standard encryption methods) and subsequently perform matching in the encrypted domain.[83] Even small differences in the values of feature sets, which are extracted from the raw biometric data, will lead to enormous differences in the resulting encrypted features. To overcome this problem one could decrypt the template and then perform matching between the query template and the decrypted reference template. However, it is demonstrated by Feng and Jain that a minutiae template (i.e. template of a fingerprint) can be reverse engineered into the original image, which may pose security risks to the biometric template, the biometric data as such and consequently the privacy of users involved.[84] Previously, scientists faced the problem of (additional) spurious minutiae generated in the reconstructed image, while these minutiae were not included in the original minutiae template. Feng and Jain have overcome this problem by creating a novel algorithm enabling the reconstruction of the fingerprint with limited spurious minutiae. The algorithm has been evaluated in respect of two categories of attacks (matching the reconstructed fingerprint against the original fingerprint and matching the reconstructed fingerprint against different impressions of the original fingerprint) by means of a commercial fingerprint recognition system.[85] Feng and Jain demonstrated that both attacks can be successfully performed using the reconstructed image. Hence, the protection of biometric data not merely comprises data storage, but also the entire process of retrieving the reference template during the authentication procedure, including the decryption of the template and the matching process.

***Ideal properties of template protection design***

As conventional encryption techniques require decryption in order to compare the query template with the reference template, which poses risks to the biometric data, they do not possess the four properties of an ideal biometric template protection design to prevent impostor attacks, and additional threats: diversity, revocability, security, and performance.[86] Diversity encompasses protection against cross matching across databases in order to guarantee the user's privacy.

---

[81] Feng and Jain demonstrated that a fingerprint template can be reconstructed into the original image, see Feng, J., Jain, A.K., "Fingerprint Reconstruction: From Minutiae to Phase" (hereinafter Feng & Jain 2011), IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 2, pp. 209-223, Feb. 2011.
[82] See section 6.1.
[83] Jain *et al* 2008, p. 6.
[84] Feng & Jain 2011; Feng (member of IEEE) and Jain (fellow of IEEE) are currently conducting research on 'Fingerprint Reconstruction From Minutiae' at the Department of Computer Science and Engineering of Michigan State University, see http://biometrics.cse.msu.edu/projects/fingerprint_reconstruct.html.
[85] Feng & Jain 2011, p. 209.
[86] Jain *et al* 2008, p. 5-6.

Revocability refers to the possibility to revoke the compromised biometric template and reissue a new template, based on the same previously provided biometric data, without the need to re-enroll. Security of templates involves protection against adversary attacks through mathematical algorithms. Performance entails the obtaining of template protection without degrading the recognition performance (FAR, FRR) of the system. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorized in *feature transformation* and the employment of a *biometric cryptosystem*.[87] Basically, feature transformation is encryption of a biometric and biometric cryptosystems generate a cryptographic key directly from or with help of the biometric (i.e. biometrically facilitated encryption). So, simply put, feature transformation and biometric cryptosystems operate reversely. Feature transformation is the most significant template protection design with respect to this thesis as it produces a yes/no response (i.e. match or non-match), as in conventional non-transformed biometric systems. Biometric cryptosystems, on the other hand, produce a cryptographic key, which technique is therefore less usable for verification and identification purposes.

Biometric systems are susceptible to several threats, such as impostor threats (e.g. identity fraud, biometric database attack, enrolment fraud, spoofing and Trojan horse attacks) and additional threats (e.g. function creep, tracking and tracing, linking of biometric data to other personal information, system failures and leakage of biometric data). Several mechanisms to overcome vulnerabilities in biometric systems are human intervention, human supervision, liveness detection and multimodal biometrics. A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorized in **feature transformation** and the employment of a **biometric cryptosystem**. Both are effective methods to protect biometric templates. Although biometric templates as such are significantly more safely compared to the use of raw biometric data, the country reports show that very few countries address the need to use templates. The Council of Europe's 2005 progress report and the 2011 Parliamentary Assembly's both recommend the use of **templates** instead of raw biometric data, but Mr Haibach's recommendations (in the 2011 report) regarding the use of templates have been noticed only in **Estonia** and **Italy**. The Estonian report underlines the importance to use biometric templates instead of raw biometric data.[88] The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects. For example, the storage of **encrypted templates** exclusively held by the data subject should be preferred over storage in central databases. Data protection legislation should include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.

[87] Jain *et al* 2008, p. 6;
[88] See Section 7.1.4 for the Estonian response to the questionnaire.

# 7 Country responses to the questionnaire

## 7.1 Responses of 22 out of 47 countries

Our questionnaire containing 7 important questions regarding the use of biometrics has been sent to 47 countries from which 23 countries responded. Portugal has been omitted from this report because it did not want its reply to be published. Therefore, this section contains the responses of 22 countries which are provided in alphabetical order in the following 22 sections. The abbreviations DPL and DPA, used in the summarised responses hereinafter, stand for Data Protection Legislation respectively Data Protection Authority. Each subsection (i.e. each country report) contains the summarised answers of the Member States that provided responses to the 7 questions of our questionnaire. The most interesting information (noted as 'Information of interest') to our report is contained in boxes at the end of each subsection.

### 7.1.1 Albania

1. No specific legislation regarding biometrics. Biometric data are addressed in data protection legislation, and considered personal data. Also provisions on biometrics in police legislation.
2. Fingerprints are used for Albanian ID cards and biometric passports
3. Not indicated
4. Not indicated
5. Yes, a fingerprint database needed for the production and issuance of citizens' identity documents, and a central biometric database for police legislation including fingerprints, facial images, and DNA samples.
6. No report that system or data have been attacked or corrupted.
7. No answer

**Information of interest**: The Albanian report underlines that the Ministry of Interior is the owner and controller of the personal data, including biometric data, needed for the issuance of ID cards and biometric passport.

### 7.1.2 Austria

1. Provisions on DNA are incorporated in police legislation and the penal procedure act. All EU regulations in this area (e.g. Eurodac regulation, and Prüm decisions) are fully implemented in different national acts.
2. The latest technical generation of identification databases, including facial images, fingerprints (AFIS – automated fingerprint identification systems) and DNA databases.
3. Only in the public sector:
   AFIS system and picture databases for police legislation and asylum
   DNA analysis and DNA database for police legislation and asylum
   Fingerprints for acquisition and storage in national passports and ID cards
4. Passports have been issued to persons who have been using a stolen identity while applying for the passport.
5. Yes, in the public sector.
6. No.
7. No such research has been conducted.

**Information of interest**: The Austrian report underlines that in accordance with Austrian law fingerprint images which have to be stored on the chip of the electronic passport have to be deleted from the database after issuing the document. In some cases passports have been issued to persons who have been using a stolen identity while applying for the passport. It is remarkable that the Austrian report states that this could have possibly been prevented if the fingerprints had been stored in a central database permanently and the passport authority had the right to use this data.

The central storage of biometric data, namely, poses more risks for function creep or linking of data to other databases.

### 7.1.3 Denmark

1. Only police legislation regarding DNA. New legislation being prepared regarding the processing of fingerprints, including rules on deletion of personal information within a central register of fingerprints.
2. State of the art IT-tools for DNA-comparison and fingerprint identification. The DNA register is currently being transformed to the CODIS system. The fingerprint identification system is being exchanged to an AFIS system.
3. The CODIS system for DNA, and an AFIS system for fingerprints.
4. No answer
5. Public databases on fingerprints and DNA, containing both identified persons, previously known for criminal activities, and crime scene traces.
6. No biometric systems were hacked or compromised.
7. Research is continuously being conducted on DNA, primarily by external authorities such as the Department of Forensic Medicine at the University of Copenhagen.

**Information of interest**: The Danish report underlines that the use of AFIS (Automated Fingerprint Identification System) will be supplemented with a number of live scanners situated around the country in specific strategic places.

### 7.1.4 Estonia

1. Yes, biometric data is regulated in national data protection legislation and considered sensitive personal data. National DNA register and national fingerprint register regulated by national legislation.
2. Biometric passports and DNA sample database. Estonia has all the most commonly used biometric technologies.
3. Public sector: biometric passports, DNA register, fingerprint register
   Private sector: fingerprint and iris scans used for security and workplace entry reasons.
4. Problems with the private sector using security systems that use biometric data (like fingerprints, palm prints or iris scans) for identifying workers. According to the Estonian Personal Data Protection Act sensitive data cannot be used for performance of a contract. For the use of biometric data for security reasons the consent of the data subject is needed. The advisor of the Estonian Data Protection Inspectorate recommends using systems that don't record the biometric image but create a code from the image and use that.
5. Yes, a national DNA register and a national fingerprint register. Both are regulated by national law.
6. No information on that matter
7. No information on that matter

**Information of interest**: The Estonian report underlines that biometric data is considered sensitive personal data in the Estonian DPL. Answer 3 mentions private sector use of biometrics (fingerprints and iris scans) for security and workplace entry reasons. The advisor of the Estonian Data Protection Inspectorate recommends the use of systems that don't store biometric images but a biometric template of that image. It can be concluded that the recommendations of Mr Haibach have been noticed in Estonia.

### 7.1.5 France

1. The processing of biometric data is regulated through DPL.
2. CNIL (Commission Nationale de l'Informatique et des Libertés; the French Data Protection Authority) has recently assessed the use of the venous networks of the hand, speech or typing

recognition, multimodal devices combining face images in two dimensions, iris scan, and speaking verification. The objectives for implementing biometric processing are changing too. Apart from classical control of access to premises or to computers, venous pattern is used for bank payment, iris and voice recognition for security of information systems, and fingerprints in a hospital to identify critically ill patients with certainty.

3. Technological developments make the CNIL's position necessary to change. For example, hand geometry was favored by the CNIL so far because it leaves no trace. But the venous system has now the same qualities and its use could be reconsidered for purposes such as working hour recordings and security of specific protected areas. The difficulty to use fingerprints combined with a centralized database still remains even though some changes have been made.
4. Palm printing, iris scan, and "hand venous pattern". Other technologies such as facial or voice recognition are still experimental.
5. The situation is changing regarding the public sector due to the evolution of the European legislation. So far CNIL was of the opinion that storage in a centralized database is only possible for biometrics with "no trace". But these are very limited data bases. Concerning fingerprints, the use of centralized databases is strictly supervised. In the private sector, the use of such databases is only allowed "for a strong security imperative" such as monitoring patients in radiotherapy in a hospital. Regarding the public sector, CNIL has always opposed to the creation of a centralized database of fingerprints by insisting on having a parliamentary debate. As a result, the government decided to give up the proposed biometric identity card which relied on the creation of a centralized fingerprints database. The first time the French government decided to implement a centralized fingerprints database was in 2009 for the application of the European Regulation 2252/2004 (EC) of 13-12-2004 on security features and biometrics in passports. Later, the government implemented a centralized biometric database for the management of its "control return assistance" policy which aims at giving financial assistance to foreigners wishing to go back to their countries. This fingerprints data base detects any new application by a person who has already benefited from this financial assistance under another identity.
6. No information on this issue.
7. Two projects have been authorized by CNIL:
   - "Technology Vision Techno-vision" is led by the University of Evry Val d'Essonne, independent public research organization. It is supported by the Ministries of Research and Defense. Its aim is to create a database and conduct multimodal assessment of recognition systems developed by other research laboratories.
   - "3DFACE" is led by Sagem Defense, a private research group, coordinated by "Sagem Défense Sécurité". It is part of the IST program (Information Technology for the Information Society) of the European Commission and brings together twelve partners in the European Union.
   CNIL does not have a report so far.

**Information of interest**: The processing of biometric data is regulated in DPL. Prior checking: biometric processing needs to be authorized by the DPA (CNIL; Commission Nationale de l'Informatique et des Libertés). Double check in the public sector: the implementation of biometrics is subject to a decree of the Council of State, adopted on the basis of the DPA's opinion.
Strict regulation and since 2004 a doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. Biometric devices are categorized upon their risks for privacy and data protection:
- "with a trace": fingerprints and palm prints. The use of these devices is considered to involve significant risks in terms of privacy. CNIL has been particularly cautious about the use of fingerprints;
- "without a trace": hand geometry, finger vein patterns;
- "intermediate": voice and face recognition, iris scan.
The CNIL considers the use of "with a trace" biometric device to be legitimate if the biometric data are stored on a storage medium under the exclusive control of the data subject, as opposed to

storage in a centralized database. In the private sector, the deployment of a centralized database should be linked to a "strong security imperative" that the CNIL will assess.
The doctrine evolves continuously due to new biometric developments and European legal developments such as Regulation 2252/2004 (EC) on biometrics passports.
In France, venous pattern technology is used for bank payments, iris recognition and voice recognition are used for security of information systems, and fingerprints in a hospital to identify critically ill patients with certainty.
The French Data Protection Authority CNIL is one of the few countries that apply prior checking.

### 7.1.6 Georgia

1. The processing of biometric data is regulated in DPL.
2. The Civil Service Development Agency uses several biometrics. Facial images for several national documents and face recognition systems. Fingerprints for travel documents (based on the ICAO recommendations) and for the automatic border crossing system ("eGate"). The Civil Service Development Agency is currently working on a document ("Seamen's book") in which the biometric fingerprint template will be introduced as a 2D barcode, based on the ILO "Seafarers' Identity Documents Convention" 2003 (No. 185).
3. The Civil Service Development Agency is using facial images and fingerprints for biometric passports and facial images for national ID cards. Both of these documents are issued by the Ministry of Justice of Georgia. Other governmental institutions are also using biometric images for their document issuance purposes. In addition, both private and public sectors are using fingerprints for access systems.
4. The Civil Service Development Agency has not encountered any problem regarding the issue.
5. The Civil Service Development Agency has a central database of biometric data, which is primarily used for citizen identification purposes.
6. No.
7. No research regarding biometrics has been conducted.

**Information of interest:** the Georgian data protection act explicitly states in Article 2(b) biometric data as a special category of data. Article 2(c) defines biometric data as any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person. Article 9 paragraph 1, on the processing of biometric data by a public institution, reads as follows: "The processing of biometric data by a public institution shall be allowed only for the purposes of the security of person and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts." Article 10, on the processing of biometric data by a private person, includes a notification obligation for the biometric system's processor. Article 10 reads as follows: "The processing of biometric data by a private person shall be allowed only if it is necessary for the purposes of conducting activities, for the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts. Before using biometric data, a data processor shall notify a personal data protection inspector detailed information on the processing of biometric data, including the information notified to a data subject, the purpose of the processing of data and the safeguards of the protection of data, unless otherwise provided by the law."

### 7.1.7 Hungary

1. Biometrics are regulated in acts on (1) genetic research and biobanks, (2) law enforcement, and (3) travelling abroad.
2. Biometric passports which include on a chip: personal data (personal identification data, signature, and facial image of the applicant) and fingerprints (protected by a special encoding) of

the holder. Fingerprints are introduced due to the mandatory provisions of Regulation 2252/2004/EC.

3. Biometric are being used in the public sector. Records of Criminal and Police Biometric Data contain fingerprint data and DNA-profile data. Main purpose of this record is the identification of potential perpetrators and suspects, deceased persons with unknown identity as well as convicted persons upon receipt into a penitentiary institution etc. Biometric passports containing digital facial images.
4. Hungary is continuously facing the penetration of biometric identification systems. In this regard petitions requesting a position on the usability of biometric entry control systems, fingerprint driven, based on cases so far, have become ever more frequent. With advances in technology, the trend of camera surveillance and using biometric entry control systems has proliferated and already reached schools. The former Data Protection Parliamentary Commissioner emphasized in several resolutions and recommendations that instead of applying biometric entry control systems which affect the privacy of the individual remarkably the use of other less intrusive methods (e.g. admission cards with magnetic stripes holding serial numbers or barcodes or other means as a replacement for biometric identification) of personal identification are advisable.
5. In the public sector: the Records of Criminal and Police Biometric Data contain fingerprint data and DNA-profile data. Main purpose of this record is the identification of potential perpetrators and suspects, deceased persons with unknown identity as well as convicted persons upon receipt into a penitentiary institution etc.
6. No information about it.
7. Not answered.

**Information of interest:** The former Data Protection Parliamentary Commissioner emphasized in several resolutions and recommendations that instead of applying biometric entry control systems which affect the privacy of the individual remarkably, the use of other less intrusive methods (e.g. admission cards with magnetic stripes holding serial numbers or barcodes or other means as a replacement for biometric identification) of personal identification are advisable.

### 7.1.8 Ireland

1. The processing of biometric data is regulated through DPL.
2. Not answered.
3. Authentication systems: identification systems and verification systems (typically storage on a card).
4. The principal difficulty across all sectors arises from attempts to introduce biometric systems without consultation with and consent of intended users (e.g. employees in the workplace).
5. No central database in Ireland.
6. There are no known incidents of hacking or compromising of biometric data in Ireland.
7. The Data Protection Commissioner has two guidance notes on his website as follows:

   Biometrics in the workplace: http://dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/bio.htm; and

   Biometrics in Schools, Colleges and other Educational Institutions: http://www.dataprotection.ie/viewdoc.asp?DocID=409.

**Information of interest:** Ireland encounters the problem of attempts to introduce biometric systems without consultation with and consent of intended users (e.g. employees in the workplace).

### 7.1.9 Italy

1. The processing of biometric data is regulated through DPL:
   - The processing of biometric data must be notified to the DPA.

- Prior checking of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects.
- The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.

In addition, Italy implemented EU legislation concerning the processing of biometric data in specific sectors or for specific requirements. In particular EU regulation defining specific standards for electronic passports, including the obligation to store two fingerprints (not templates thereof) in the relevant chip in order to allow identity verification. Furthermore EU regulation establishing huge EU databases containing biometric data (e.g. Eurodac, and VIS).

2. The processing of graphometric data is becoming more widespread for the secure signature of documents, mainly in the banking and insurance sectors and in connection with utilities. A few biometrics-based techniques are used (not on a regular basis) in connection with IT-authentication procedures, which are envisaged as minimum security measures. Fingerprints are mostly relied upon. Hand contour and/or fingerprints are used in some cases for physical access control. The processing of video surveillance data is performed for the recognition of bodily traits for physical access control, mainly in the banking sector (anti-robbery and anti-camouflage checks). The processing and analysis of genetic data are offered also online on a 'do-it-yourself' basis.
3. Biometric systems in the workplace, in particular for the control of employees' access to workplace areas. Other cases concern the use of biometrics for access to banks, sports centres, and schools. In 2008, the Italian DPA laid down specific recommendations and measures with regard to the Ministry of Interior's 'Guidelines on the collection of fingerprints of members of the country's Roma community'. Other databases containing biometric data are those related to Eurodac and VIS. Moreover, the Italian immigration law requires the collection of fingerprints of all aliens entering the territory as well as for requiring/renew the permit to stay. Fingerprints of foreigners including those of asylum seekers are stored in the national AFIS which is operated by the Scientific Police. Biometric systems based on fingerprints are used with regard to biometric passports in which fingerprints are stored locally on the chip.
4. The main difficulties regarding the application of data protection principles are:
   - The proportionality principle and the purpose specification principle. The Italian DPA recently found that the processing of biometric data to regulate access to a sports centre was disproportionate.
   - The criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent).

   The DPA issued several decisions regarding the use of biometrics in the workplace. The main principles of the DPA in the workplace context are as follows:
   - 1) The blanket, unrestricted use of biometric data is not permitted. On account of their nature, these data require specific precautions to prevent harming data subjects. Therefore, as a rule it is not permitted to process fingerprint data to control the number of hours worked by the employees.
   - 2) Using biometric data may only be justified in specific cases by taking account of the relevant purposes and context in which data are to be processed. This is the case, for example, if access to "sensitive areas" is to be regulated through the use of biometrics.
   - 3) Biometric verification and identification systems based on the reading of fingerprints stored as encrypted templates on media that are held exclusively by the relevant data subject should be preferred over centralised processing of biometric data.
5. Biometric databases set up by the police. Biometric systems in the workplace, in particular for the control of employees' access to workplace areas. Other cases concern the use of biometrics for access to banks, sports centres, and schools. Other databases containing biometric data are those related to Eurodac and VIS. Moreover, the Italian immigration law requires the collection of fingerprints of all aliens entering the territory as well as for requiring/renew the permit to stay. Fingerprints of foreigners including those of asylum seekers are stored in the national AFIS

which is operated by the Scientific Police. Biometric systems based on fingerprints are used with regard to biometric passports in which fingerprints are stored locally on the chip.
6. No personal data breaches caused by biometric technologies.
7. Not answered.

**Information of interest:** (1) the processing of biometric data must be notified to the DPA. (2) Prior checking of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects. (3) The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.
The Italian DPA faces difficulties regarding the application of data protection principles, in particular the proportionality principle, the purpose specification principle, and the criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent).
The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects: (1) no unrestricted use, (2) justification grounds taking into account the relevant purposes, and (3) storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases.
In 2008, the Italian DPA laid down specific recommendations and measures with regard to the Ministry of Interior's 'Guidelines on the collection of fingerprints of members of the country's Roma community'.

### 7.1.10 Lithuania

1. No separate legal act which regulates all biometric data processing. The processing of fingerprint data in a fingerprint register is regulated by law enforcement legislation.
2. Not answered.
3. Public and private bodies mostly use video surveillance systems. Also the Lithuanian DPA (SDPI; State Data Protection Inspectorate of the Republic of Lithuania) has encountered questions regarding the possibility to use fingerprint data in the private sector (e.g. gyms, schools, and university dormitory for entrance purposes), but after the consultation with the DPA such systems (except university dormitory) are not deployed because the DPA issued a prohibition order to use such systems. One firm issuing certificate for the IT specialists, have proved necessity to use vein pattern in order to identify person taking the exam for the certificate, because the certificate is widely acknowledged and for them it was important to prevent fraud attempt at the exam. The DPA also encountered the plan of the Lithuanian State Social Insurance Fund Board to implement a voice recognition system as one of the alternatives for the identification of insured persons in order to provide personal data to him by phone. The Lithuanian DPA is still examining this plan.
4. Due to the fact that legislation does not state whether biometric data should be regarded as sensitive data, data controllers processing biometric data do not have legal certainty whether prior checking (provided in Lithuanian DPL) shall be carried on or not. Legal uncertainty is also caused by the lack of legislation on biometric data processing and the lack of clear requirements on such processing.
5. There is only one fingerprint register at the Lithuanian police. The Lithuanian DPA has no information on the existence or planning of other central biometric databases in the public or private sector.
6. The Lithuanian DPA is not aware of such situations.
7. The Lithuanian DPA is not aware of such research or reports.

**Information of interest:** The Lithuanian DPA (SDPI; State Data Protection Inspectorate of the Republic of Lithuania) has encountered questions regarding the possibility to use fingerprint data in the private sector (e.g. gyms, schools, and university dormitory for entrance purposes), but after the

consultation with the DPA such systems (except university dormitory) are not deployed because the DPA issued a prohibition order to use such systems. One firm issuing certificate for the IT specialists, have proved necessity to use vein pattern in order to identify person taking the exam for the certificate, because the certificate is widely acknowledged and for them it was important to prevent fraud attempt at the exam. Due to the fact that legislation does not state whether biometric data should be regarded as sensitive data, data controllers processing biometric data do not have legal certainty whether prior checking (provided in Lithuanian DPL) shall be carried on or not. Legal uncertainty is also caused by the lack of legislation on biometric data processing and the lack of clear requirements on such processing.

### 7.1.11 Macedonia

1. Macedonian DPL states biometric data as a special category of personal data. Prior checking by the Macedonian DPA, prior to the processing of biometric data necessary to confirm the identity of the data subject.
2. Not answered.
3. From the received requests for obtaining the approval for processing biometric data, the Macedonian DPA concludes that the most frequent requests are for biometric systems that are processing fingerprints.
4. One of the problems encountered with regard to the processing of biometric data (in both the public and private sector) is the intention of controllers to use the biometric system to control employees, to prove the presence of the employees. This controllers' intention is due to the fact that a biometric system is one of the cheapest ways to control employees, cheaper than the system for performing video surveillance. Therefore, the Macedonian DPA required the controller to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.
5. One of the central registers for biometric data in the Republic of Macedonia is in the Ministry of interior and it is for providing data for issuing passports and personal ID cards.
6. The Macedonian DPA is not aware of or informed by the Ministry of Interior on the hacking or compromising of biometric systems.
7. The Macedonian DPA is not aware of research on biometrics.

**Information of interest:** the Macedonian DPL states biometric data as a special category of personal data. Prior checking by the Macedonian DPA, prior to the processing of biometric data necessary to confirm the identity of the data subject. One of the problems encountered with regard to the processing of biometric data (in both the public and private sector) is the intention of controllers to use the biometric system to control employees, to prove the presence of the employees. This controllers' intention is due to the fact that a biometric system is one of the cheapest ways to control employees, cheaper than the system for performing video surveillance. Therefore, the Macedonian DPA required the controller to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.

### 7.1.12 Malta

1. Malta does not have regulation or legislation with regard to biometrics.
2. The latest biometric technologies available are voice, fingerprint, and hand palm recognition devices, iris scanners, and face geometry devices.
3. The devices currently being used are the fingerprint and hand palm recognition devices. In both private and public sectors these are used for time and attendance verification, payroll purposes, general administration and for access to specific designated areas. In the public sector these are also set for the issue of biometric passports.

4. No specific problems or difficulties have been encountered in both the private and public sectors with regard to biometrics. When they were first introduced trade unions had voiced their concern on the legality or otherwise of the installation of such devices at the place of work and to date they seek the advice of the Maltese DPA on any queries on this matter.
5. One example of a central database in the public sector is 'NIDMS – National Identity Data Management System'. This records biometric data (fingerprints) for passport and issuance of VISA purposes. The Maltese DPA is not aware of any central database in the private sector.
6. The Maltese DPA is not aware of any situations were biometric systems were hacked or compromised.
7. The Maltese DPA issued a paper entitled 'The Use of Biometrics Devices at the Workplace'.

**Information of interest:** -

### 7.1.13 Monaco

1. The processing of biometric data is regulated through the Monegasque DPL.
   Prior checking: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorization from the Monegasque DPA (CCIN; Commission de Contrôle des Informations Nominatives).
   Penalisation: "persons who, knowingly, collect or cause to be collected, record or cause to be recorded, store or cause to be stored, use or cause to be used personal data relating to suspected unlawful activities, offences, security measures or including biometric data that is required to check persons' identities or is intended for the purposes of surveillance without having obtained the authorization laid down in Article 11-1", "[…] shall be punished by imprisonment for three months to one year and by a fine as described in item 4 of Article 26 of the Criminal Code or only one of those two penalties".
2. Private sector: Biometric systems which can recognise the contour of the hand, the venous network of the fingers of the hand, and fingerprints.
3. Private sector: biometric systems are being used for access control and time attendance of employees. The Commission excluded the use of systems based on fingerprint recognition for the purpose of time management, time attendance of employees, and for access control at entrances and exits of companies or organisations, because they present a greater risk to individuals than systems based on recognition of the contour of the hand or finger vein patters of the hand. Biometric devices that have been analysed since 2011 by the supervisory authority raised no particular difficulty. The controllers of these systems have met the principles set out in the supervisory authority's recommendations.
   Public sector: biometric data are used in the police database AFIS. Data from DNA samples from crime scenes or suspects or defendants are included in the court records, but not contained in the database. Biometric data are used for identity cards, including two fingerprints and a digital photograph. These data are stored in the computer system used for the issuance of identity cards and cannot be interconnected with any other file. It has never been compromised.
4. Private sector: problems have been encountered regarding two biometric devices. By Resolution no. 2010-19 of 26 May 2010, published on the website of the CCIN, the Commission issued an opinion unfavourable to the implementation of systems based on fingerprint recognition with the purpose of securing access control. The system was deployed in a cloakroom. The Commission noted that the deployment was disproportionate and the system lacked security measures. During an investigation conducted on 14 March 2011, the Commission staff noted the existence of an unsecured central database for fingerprints for which no approval had been granted. The use of both biometric systems had been stopped at the request of the Commission.
5. Not answered.
6. Not answered.
7. Not answered.

**Information of interest:** the Monegasque DPA prohibits the use of biometric systems based on fingerprints in the workplace. The DPA supervises security requirements applicable to biometric systems and the prohibition of the further use of biometric data. Prior checking: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorization from the Monegasque DPA (CCIN; Commission de Contrôle des Informations Nominatives). Penalisation: "persons who, knowingly, collect or cause to be collected, record or cause to be recorded, store or cause to be stored, use or cause to be used personal data relating to suspected unlawful activities, offences, security measures or including biometric data that is required to check persons' identities or is intended for the purposes of surveillance without having obtained the authorization laid down in Article 11-1", "[…] shall be punished by imprisonment for three months to one year and by a fine as described in item 4 of Article 26 of the Criminal Code or only one of those two penalties".

### 7.1.14 Montenegro

1. The processing of biometric data is regulated through the Montenegrin DPL. Biometric data is defined as '[…] data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly". Prior checking: prior to the processing of biometric data, the approval of the Montenegrin DPA is required, because the processing represents a particular risk for the rights and freedoms of individuals. The processing of biometric data is only allowed if it is provided for by law and in accordance with the law. Biometrics are only allowed if it is "[…] necessary for the protection of individuals and property or for the protection of secrecy of data or business secrets […]" when there are no other authentication methods, if is obligated by international treaties, or to establish the identity of individuals crossing the state borders.

   The Montenegrin Code of Criminal Procedure contains provisions regarding the 'examination, autopsy and exhumation of a corpse' and the 'physical examination and other procedures' in which the use of DNA is regulated.
2. No information provided.
3. No information provided.
4. No information provided.
5. Montenegro does not have a central database for biometric data. However, it has a database containing the fingerprints of two fingers which are collected in the context of legislation on identity cards. Additionally, the police has a database for biometric data (the answer of Montenegro does not elaborate on this issue). Montenegro does not yet have a DNA register, although required by law.
6. No problems regarding hacked or compromised biometric systems.
7. No information provided.

**Information of interest:** Biometric data is defined as '[…] data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly". Prior checking: prior to the processing of biometric data, the approval of the Montenegrin DPA is required, because the processing represents a particular risk for the rights and freedoms of individuals.

### 7.1.15 Netherlands

1. Criminal law: yes, specific provisions regulate the collection of facial images and fingerprints.
   Travel documents: yes, the Dutch Passport Act regulates the storage of facial images and fingerprints in the passport. The Passport Act also regulates the storage of two fingerprints in a decentralised storage register, operated by the individual municipalities. The 2009 amendment

of the Dutch Passport Act[89] contains a provision on the travel document administration which is intended to include the central storage of fingerprints.[90] This provision on the travel document administration has, in contrast to the provision on the storage of biometrics in passports, not yet entered into force.
A recently proposed amendment of the Dutch Passport Act[91] aims at (1) ceasing from the storage of fingerprints, (2) ceasing from the storage of fingerprints in Dutch identity cards, and at (3) collecting two instead of four fingerprints when someone applies for a passport.

2. Criminal law: facial images and fingerprints are primarily being used for identification purposes during criminal proceedings.
   Travel documents: for the application and issuance of Dutch travel documents devices to collect fingerprints and devices to digitalise a facial image and signature are being used.
3. Criminal law: facial images and fingerprints to (1) identify suspects and convicts, and for (2) criminal investigation purposes.
   Travel documents: for the application and issuance of Dutch travel documents biometric devices to collect and verify fingerprints, and specific technology to digitalise facial images are being used.
4. Criminal law: problems regarding the (1) technology (e.g. stability and performance), the (2) operation of the fingerprint device, and the (3) quality of the fingerprints (e.g. technical problems and organizational problems).
   Travel documents: with regard to facial images in Dutch travel documents no major problems have been occurred. There is, however, social resistance regarding the storage of fingerprints as there are doubts about the need to store fingerprints, and about the efficacy of using fingerprints.
5. Criminal law: yes, a national fingerprint database (called HAVANK) for criminal investigation purposes (the identification of suspects, convicts, and witnesses) operated by the Dutch police. The facial images collected for the same purposes are processed in the database operated by the Dutch criminal courts. Facial images and fingerprints being used in Dutch prisons and institutions for people who committed a crime and suffer from a mental disorder, are processed in a biometric database.
   Travel documents: no.
6. Criminal law: no, but there have been situations in which users tried to spoof a biometric system.
   Travel documents: no.
7. Criminal law: several Dutch universities, including Tilburg University, have conducted research on biometrics.
   Travel documents: attached a 2012 report on the decision making process of the Dutch government with regard to biometrics in Dutch travel documents.

The Dutch independent foundation Privacy First recently presented its 2012 annual report.[92] Privacy First's aim is to preserve and promote the right to privacy and a free society with a central focus on biometrics. Its 2012 annual report shows the issues Privacy First is concerned

[89] *Staatsblad* 2009, 252. The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published.
[90] The intention to include, *inter alia*, fingerprints in a central database is noted in the Explanatory Memorandum, see *Kamerstukken II* 2007/08, 31 324, No. 3, p. 34. The *Kamerstukken* are Parliamentary Documents. "II" refers to the Second Chamber. The document referred to can be found at https://zoek.officielebekendmakingen.nl/, by searching the series number, in this case 31324. The Article referred to in the Explanatory Memorandum and containing the provision on the travel document administration ("*reisdocumentenadministratie*") is Article 4a of the amended Dutch Passport Act [Staatsblad 2009, 252].
[91] *Kamerstukken II* 2012/13, 33 440, No. 2.
[92] The 2012 Annual Report (in Dutch), Privacy First Foundation, Amsterdam, 29 March 2013, http://www.privacyfirst.nl/images/stories/PDFs/jaarverslag_privacyfirst_2012.pdf.

about, such as privacy issues about biometrics regarding the Dutch Passport Act and the access to centralised and decentralised fingerprint databases by Dutch and foreign secret services.

**Information of interest:** The 2009 amendment of the Dutch Passport Act[93] contains a provision on the travel document administration which is intended to include the central storage of fingerprints.[94] This provision on the travel document administration has, in contrast to the provision on the storage of biometrics in passports, not yet entered into force.
With regard to facial images in Dutch travel documents no major problems have been occurred. There is, however, social resistance regarding the storage of fingerprints as there are doubts about the need to store fingerprints, and about the efficacy of using fingerprints. A recently proposed amendment of the Dutch Passport Act[95] aims at (1) ceasing from the storage of fingerprints, (2) ceasing from the storage of fingerprints in Dutch identity cards, and at (3) collecting two instead of four fingerprints when someone applies for a passport. Problems with biometric systems used in the context of criminal law enforcement have been encountered regarding the (1) technology (e.g. stability and performance), the (2) operation of the fingerprint device, and the (3) quality of the fingerprints (e.g. technical problems and organizational problems).

### 7.1.16 Niger

1. Niger does not have any legislation on biometric data, although by 2015 Niger hopes to introduce biometric passports and hopes to have a biometric electoral roll.
2. Not answered.
3. Not answered.
4. Not answered.
5. Not answered.
6. Not answered.
7. Not answered.

**Information of interest:** -

### 7.1.17 Poland

1. No general regulation/legislation with regard to biometrics. Biometric databases are set up on the basis of specific provisions, which specify the tasks and powers of particular authorities (e.g. border guard and military police). Access to biometric data collected by such entities is possible only for authorised, strictly specified authorities, in connection with the conducted proceedings. Poland has two acts in which biometrics are regulated: the Act on Passport Documents and the Act on the Police, which contains provisions on a fingerprint database (CRD; Central Dactyloscopic Registry) and on a DNA database.
2. In Poland, the latest biometric technologies solutions are being implemented. Bank PBS (Bank Polskiej Spółdzielczości) has already exchanged over 90 per cent of its cash machines for devices in which finger vein scan is a transaction confirmation. Wincor-Nixdorf biometric cash machines

[93] *Staatsblad* 2009, 252. The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published.
[94] The intention to include, *inter alia*, fingerprints in a central database is noted in the Explanatory Memorandum, see *Kamerstukken II* 2007/08, 31 324, No. 3, p. 34. The *Kamerstukken* are Parliamentary Documents. "II" refers to the Second Chamber. The document referred to can be found at https://zoek.officielebekendmakingen.nl/, by searching the series number, in this case 31324. The Article referred to in the Explanatory Memorandum and containing the provision on the travel document administration ("*reisdocumentenadministratie*") is Article 4a of the amended Dutch Passport Act [Staatsblad 2009, 252].
[95] *Kamerstukken II* 2012/13, 33 440, No. 2.

using Hitachi Finger Vein technology were applied by this bank. The Institute of Mathematical Machines issued an official opinion on innovation in relation to the Finger Vein solution destined for cash machines and bank affiliates. The opinion concerns a solution based among others on Finger Vein (HOTS 609) bank readers and FVS software. Thanks to this opinion a bank in Poland which purchases Finger Vein solution will be able to apply for tax refund in the amount of 50 per cent of the cost of purchased solution. Finger Vein is the only biometric technology having such opinion on innovation.

3. In Poland the following biometric identification systems are applied:
   - Automated Fingerprint Identification System (AFIS) - kept by the Police;
   - Cash machine authorization systems, where biometric data are used to scan finger vein as authentication system in cash machines. This technology is used e.g. by the bank "Bank Polskiej Spoldzielczosci S.A."
   - CRD (Central Dactyloscopic Registry) – information in the form of fingerprints collected and obtained by the Police is processed in this central data filing system;
   - Central Register of Issued and Annulled Passports – in this data filing system among others the following data are processed: face images (photographs) and fingerprints;
   - Passport System of the Ministry of Foreign Affairs – in this data filing system among others the following data are processed: face image and fingerprints;
   - Eurodac module within the IT system "Residence" – in this module fingerprints are processed, in connection with the need to identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the European Union;
   - DNA Database, kept by the Police – in this data filing system among others the following data are processed: data revealing directly or in context genetic code;

   Please, note that automated exchange of DNA data from fingerprints databases and DNA databases also takes place through the agency of INTERPOL as well as within the framework specified by the Prüm Decision (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime).

   - Moreover, biometric data are used (contrary to the Polish law) in the working time monitoring systems by some entities (see point 4 as regards this problematic issue); or in buildings or rooms access control systems;

4. One of the problems related to implementation of biometric technologies is a closed catalogue containing employee data which can be processed by an employer in connection with employment. The catalogue does not include biometric data and therefore there is no legal basis for using biometric technologies in working time monitoring systems. In a few cases solutions applied for this purpose were reported by employees as illegal, and court decisions were issued ordering the removal of these solutions.
   Another problem connected with implementation of biometric technologies is the lack of official definition of biometric data and distinguishing biometric data processed in the form of electronic record, which are used in IT solutions, from traditional ones, such as personal signature, face image photograph or voice.
5. Yes, a Central Dactyloscopic Registry (CRD), containing fingerprints collected by the police, and an Automated Fingerprint Identification System (AFIS), operated by the police.
6. No situations of hacking or compromising are known. However, there were cases of unauthorised use of biometric data in the work place setting to monitor working time.
7. In Poland, research regarding biometrics is conducted by the Warsaw University of Technology (Biometrics and Machine Learning Group at the Faculty of Electronics and Information Technologies) and Research and Academic Computer Network (NASK Biometrics Laboratory). Activity of Biometric Laboratory of NASK is centered on security of biometric applications,

original biometrics technologies, biometrics applications in identity recognition, remote biometrics authentication, and biometric-related smart cards.

The original solutions include access control systems based on iris recognition algorithms, as well as payment transaction verification systems based on handwritten signature analysis. Biometrics security research is centered on testing level aliveness detection level of biometric equipment, development of presentation attacks detection methods, as well as in combining cryptography and biometrics to protect biometric templates. NASK's original combination of biometrics, smart card technology and remote authorization methodology allows to create secure remote authorization mechanisms. The expertise extends also to equipment selection procedures depending on the required level of security and reliability, as well as on the given target environment.

The lab keeps an US patent related to iris aliveness detection. It also developed the world's only multimodal data base containing measurements of numerous biometric characteristics (iris, fingerprint, face, palm geometry and handwritten signature) collected over a long period of time (over 7 years) from several hundred individuals. The NASK Biometrics Laboratory actively participates in biometric standardization, being a member of Polish Committee on Standardization and ISO/IEC SC37.

The research conducted at the Warsaw University of Technology and NASK are managed by Prof. Andrzej Pacut. Also other research centres in Poland are involved in the research, including:

- Lodz University of Technology - Prof. Krzysztof Ślot (with a team),
- AGH University of Science and Technology - Prof. Khalid Saeed (with a team),
- Silesian University of Technology - Prof. Andrzej W. Mitas (with a team),
- Institute of Mathematical Machines - Mr Krzysztof Dzik (with a team)

**Information of interest:** the Polish bank PBS has exchanged over 90 per cent of its cash machines for devices in which a finger vein scan is a transaction confirmation. Poland encounters problems with regard to the deployment of biometric systems in work place settings, while there is no legal basis for using these systems to monitor working time. Other problems encountered are the lack of an official definition of biometric data and the difficulty to distinguish biometric data from other personal data. In Poland, research is conducted on: access control through iris recognition, payment transaction verification systems based on handwritten signature analysis, aliveness detection, combining cryptography and biometrics to protect biometric templates, smart card technology, and remote authorization methodology. The NASK Biometrics Laboratory holds a US patent on iris aliveness detection, and actively participates in biometric standardization, being a member of the Polish Committee on Standardization and ISO/IEC SC 37.

### 7.1.18 Portugal

Portugal has been omitted from this report because it did not want its reply to be published.

### 7.1.19 Romania

1. Biometrics are regulated in regulation on travel documents. Romanian passports contain the facial image and two fingerprints of the data subject.
2. Not answered.
3. Not answered.
4. Not answered.
5. In the public sector, a central biometric database is used for the issuance of travel documents.
6. No information on compromised biometric systems was registered.
7. No research on biometrics has been conducted.

**Information of interest:** -

### 7.1.20 Senegal

1. No legislation specifically relating to biometrics. However, legislation regarding ID cards regulates the use of biometrics (i.e. fingerprints and facial image). These biometric are used to identify citizens, and in electoral matters, to prevent multiple entries on the electoral roll. The Senegalese DPL regulates the processing of personal data in general, and the processing of biometric data in particular, which is under the control of the Senegalese DPA.
2. Biometrics recognition systems for fingerprints, facial images, iris scans, and hands/fingers.
3. Biometrics in the public sector are only be used for the purposes of the identity card and the biometric passport.
4. Not answered.
5. The Senegalese Ministry of the Interior holds a database of digital passports. In addition, a foreign company (Securiport LLC) has set up a database of passengers in Senegalese airports.
6. Not answered.
7. Not answered.

**Information of interest:** fingerprints and facial images are used in electoral matters, to prevent multiple entries on the electoral roll.

### 7.1.21 Serbia

1. No specific regulation regarding biometrics. The processing of biometric data is addressed in legislation on identity documents, state border protection legislation, police law, and criminal procedure law.
2. Facial images (FIIS; Face Image Identification System), fingerprints (AFIS; Automated Fingerprint Identification System), signature biometrics, voice identification and DNA.
3. Public sector: the Ministry of Interior operates an AFIS system, FIIS system, and DNA database. At border crossings and checkpoints Serbia employs devices able to read biometric identification documents.
   Private sector: biometric systems are used in the workplace to monitor the number of hours worked by the employees. However, due to the violation of data protection legislation the further processing of biometric data was prohibited.
4. Due to the lack of regulation concerning biometrics, many controllers in the private sector deploy fingerprint identification systems to monitor the number of hours worked by the employees. However, the Serbian DPA observed that this type of processing is disproportionate to its purpose and issued therefore warnings to several data controllers.
5. Yes. Biometric records are located in two separate databases.[96]
6. No information about it.
7. No information about it.

**Information of interest:** in addition to biometric data such as facial images, prints of all fingers and palm prints also other characteristic features of perpetrators such as tattoos and scars are being collected.

### 7.1.22 Slovenia

1. Yes. The use of biometrics in both the public and private sector is regulated in Slovenian DPL, and with regard to biometric passports in specific legislation on passports.
2. The vast majority of biometrics used in Slovenia processes fingerprints, probably exceeding 95 % market share. Given that Slovenian DPL requires prior checking before biometric measures are

[96] The answer does not clarify what kind of databases is meant.

introduced, there were only a few examples where other methods were used, i.e. face recognition and palm recognition. All in all the Information Commissioner has issued roughly 80 decisions about biometric measures since 2005, around three out of four were positive. Cases where applicants were not given permission were mostly because the applicants could not meet the legal preconditions and wanted to use biometric measures only for its ease of use or economic reasons. In terms of passports the Republic of Slovenia introduced second generation biometric passports in June 2009 (first generation that used biometric images were introduced in 2006). Second generation passports require both biometric images and fingerprints.[97]

3. Most implementations use centralized storage of biometric templates, very few were encountered where templates are stored on portable media in possession (only) of the individual. In the case of biometric passports it has to be noted that there is no centralized database – biometric data are stored only in the passport.

   In terms of purposes biometrics are mostly used for access control, e.g. to protect access to server rooms, vaults, premises with confidential information and valuable equipment or resources. There are however large tendencies to use biometric measures also for the purposes of time attendance in both private and public sector, due to the fact that biometric equipment has become easily available and also affordable. Such use however does not meet the legal preconditions. The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures may only be introduced if they are necessarily required for the *performance of activities*, for *the security of people* or *property*, or to *protect secret data* or *business secrets*. Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.

   In terms of biometric passports, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

4. In administrative procedures of applying for a decision to allow biometric measures several applicants underestimate the strictness of legal conditions. Many want to introduce biometric measures just for its ease of use or economic reasons and do not explore biometric measures for improving their security mechanisms. Many applicants have in past also been misled by biometric resellers about the effectiveness and downsides of use of biometric measures, where only the perceived benefits were presented to them. Resellers obviously tend to see the existing regulations as to strict. The opinion of the Information Commissioner is contrary and it supports the legislator's decision to limit the use of biometric measures to situations where this is absolutely necessary and where milder measures are not possible.

   There have been very few implementations where privacy enhancing technologies were used, e.g. use of template-on-card solutions etc.

5. There is no such database. Regarding biometric passports there is no centralized database; biometric data are stored only in the passport. In terms of DNA there were some proposals by some political parties in 2006 to introduce a nation-wide DNA database, but these plans were not taken on board.
6. We have not been informed about such cases. On the other side in some cases there were reports of:
   - problems with enlisting all employees (e.g. workers with damaged fingerprints)
   - problems with malfunctioning of the equipment (false acceptance/false rejections)
   - complaints and resistance by employees to be subjected to such measures.
7. Unfortunately, we are not aware of such research on national level.

**Information of interest:** the Slovenian DPL requires prior checking before biometric measures are introduced. The Information Commissioner has issued about 80 decisions about biometric measures since 2005, around three out of four were positive. Cases where applicants were not given permission to use biometrics were mostly because the applicants could not meet the legal preconditions and wanted to use biometrics measures only for its ease of use or economic reasons,

[97] The authors of this report have another definition of second generation biometrics (see section 0). According to them, biometric images and fingerprints are both considered first generation biometrics.

and do not explore biometric measures for improving their security mechanisms. Many applicants have also been misled in the past by biometric resellers about the effectiveness and downsides of the use of biometric measures, where only the perceived benefits were presented to them. Resellers tend to see the existing regulations as to strict. The opinion of the Slovenian DPA is contrary and it supports the legislator's decision to limit the use of biometric measures to situations where this is absolutely necessary and where milder measures are not possible.
With regard to biometric passports, the biometric data to be used are stored only in the passport; there is no central biometric database. Biometrics are mostly used for access control (e.g. to protect access to server rooms, vaults, premises with confidential information and valuable equipment or resources), but there is a tendency to use biometric measures also for the purposes of time attendance in both the private and public sector, due to the fact that biometric equipment has become easily available and also affordable. Such use, however, does not meet the legal preconditions.
The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures may only be introduced if they are necessarily required for the *performance of activities*, for *the security of people* or *property*, or to *protect secret data* or *business secrets.* Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.

### 7.1.23 Switzerland

1. Private sector: no specific regulation regarding biometrics. Biometric data must be processed in accordance with Swiss DPL.
   Public sector: yes, several legislative instruments.[98]
2. The Swiss DPL does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the current state of technology.
3. The Swiss DPL does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the current state of technology.
4. Today, biometric systems are available at low costs. Therefore, in the private sector the technology is often used without the need for a strong identification or any other serious reason. Subsequently, the Swiss DPA is often confronted with questions concerning the proportionality of the use of such systems; especially if a central database is part of the system. Furthermore, it is our observation that serious tensions between employer and employee can arise as soon as the employer collects the biometric data of his employees, even against their will.
5. Private sector: the Swiss DPL does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the use of central databases.
   Public sector: yes, two biometric databases. One database is set up in accordance with regulation on 'police identification'[99]. Another database 'serves as a basis for the biometric passport'[100].
6. Unknown.
7. Unknown.

**Information of interest:** in the private sector biometric technology is often used without the need of identification or any other serious reason. The Swiss DPA is often confronted with questions about the proportionality of the use of biometric systems, especially if a central database is part of the system. The Swiss DPA notices the possibility of serious tensions between employer and employees if the employer collects the biometric data of his employees, even against their will. Switzerland has two central biometric databases in the public sector.

[98] The Swiss response does not elaborate on the content of their reported legislative instruments.
[99] It is not clear what exactly is meant by 'police identification'.
[100] Although it is not clear what exactly is meant by 'serves as a basis for the biometric passport', Switzerland seems to have a central biometric database in which biometric data needed for the biometric passport is stored.

## 7.2 Main results from the questionnaire

The authors of this report have drafted 7 significant questions about the current legislation and regulation on biometrics and regarding the current state of biometric technology, (central) biometric databases, and problems arising from the deployment of biometric systems. The questionnaire was sent to 47 countries of which 22 responded. The responses differ considerably in the amount of information provided and the way in which the countries have made progress in legislation and regulation specifically aimed at the protection of biometric data. This section discusses the most interesting information in the country responses.

### 7.2.1 Countries which have adopted legislation and regulation specifically aimed at the protection of biometric data

Only few countries have adopted legislation specifically aimed at the protection of biometric data. These countries are:

- **Estonia:** biometric data is considered sensitive personal data in the Estonian DPL.

  (Interesting opinion Estonian DPA: the advisor of the Estonian Data Protection Inspectorate recommends the use of systems that don't store biometric images but a biometric template of that image.)
- **France:** France is pioneering the field of data protection in general and biometric data in particular. The processing of biometric data is regulated in French DPL, which contains a provision on prior checking: biometric processing needs to be authorized by the French DPA (CNIL; Commission Nationale de l'Informatique et des Libertés). In the public sector a double check has to be carried out: the implementation of biometrics is subject to a decree of the Council of State, adopted on the basis of the DPA's opinion.
  France has strict regulation and since 2004 a doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. Biometric devices are categorized upon their risks for privacy and data protection:
  - "with a trace": fingerprints and palm prints. The use of these devices is considered to involve significant risks in terms of privacy. CNIL has been particularly cautious about the use of fingerprints;
  - "without a trace": hand geometry, finger vein patterns;
  - "intermediate": voice and face recognition, iris scan.

  The CNIL considers the use of "with a trace" biometric device to be legitimate if the biometric data are stored on a storage medium under the exclusive control of the data subject, as opposed to storage in a centralized database. In the private sector, the deployment of a centralized database should be linked to a "strong security imperative" that the CNIL will assess.
  The doctrine evolves continuously due to new biometric developments and European legal developments such as Regulation 2252/2004 (EC) on biometrics passports.
- **Georgia:** Georgia is particularly pioneering the field of biometric data protection.
  The Georgian data protection act explicitly states in Article 2(b) biometric data as a special category of data.
  Article 2(c) defines biometric data as any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person.
  Article 9 paragraph 1, on the processing of biometric data by a public institution, reads as follows: "The processing of biometric data by a public institution shall be allowed only for the purposes of the security of person and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts."
  Article 10, on the processing of biometric data by a private person, includes a notification obligation for the biometric system's processor. Article 10 reads as follows: "The processing of biometric data by a private person shall be allowed only if it is necessary for the purposes of

conducting activities, for the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts. Before using biometric data, a data processor shall notify a personal data protection inspector detailed information on the processing of biometric data, including the information notified to a data subject, the purpose of the processing of data and the safeguards of the protection of data, unless otherwise provided by the law."

- **Italy:** several strict provisions are contained in the Italian DPL:
  - The processing of biometric data must be notified to the DPA
  - Prior checking of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects.
  - The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.

  (Interesting opinion Italian DPA: the Italian DPA faces difficulties regarding the application of data protection principles, in particular the proportionality principle, the purpose specification principle, and the criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent). The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects: (1) no unrestricted use, (2) justification grounds taking into account the relevant purposes, and (3) storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases.)
- **Macedonia:** biometric data is considered a special category of personal data in the Macedonian DPL. Prior checking by the Macedonian DPA, prior to the processing of biometric data necessary to confirm the identity of the data subject. The Macedonian DPA required the controller of biometric systems to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.
- **Monaco:** prior checking: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorization from the Monegasque DPA (CCIN; Commission de Contrôle des Informations Nominatives).
- **Montenegro:** in the Montenegrin DPA, biometric data is defined as '[…] data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly". Prior checking: prior to the processing of biometric data, the approval of the Montenegrin DPA is required, because the processing represents a particular risk for the rights and freedoms of individuals.
- **Slovenia:** the use of biometrics in both the public and private sector is regulated in Slovenian DPL. The Slovenian DPL requires prior checking before biometric measures are introduced. The main reason that the Slovenian DPA did not give permission to use biometrics is that applicants for such systems could not meet the legal preconditions and wanted to use biometrics measures only for its ease of use or economic reasons, and do not explore biometric measures for improving their security mechanisms. The opinion of the Slovenian DPA is to limit the use of biometric measures to situations where this is absolutely necessary and where milder measures are not possible.

  The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures may only be introduced if they are necessarily required for the *performance of activities*, for *the security of people* or *property*, or to *protect secret data* or *business secrets*. Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.

8 out of 22 Member States which responded to our questionnaire have adopted legislation specifically aimed at the protection of biometric data. These countries are: **Estonia**, **France**, **Georgia**, **Italy**, **Macedonia**, **Monaco**, **Montenegro**, and **Slovenia**. The provision included most often in data protection legislation of these Member States concerns prior checking. Prior checking is contained in data protection legislation of the following Member States: **France**, **Italy**, **Macedonia**, **Monaco**, **Montenegro**, and **Slovenia**. The Member States addressing biometric data as a special category of personal data are: **Georgia** and **Macedonia**. In **Estonia** biometric data is considered sensitive personal data. The Member States which adopted a definition of biometric data are: **Georgia** and **Montenegro**.

### 7.2.2 Biometrics in the contexts of sports, school and workplace

The country responses show that the main difficulties of using biometrics are being encountered in the contexts of sports, school and workplace. The countries referring to these contexts are addressed hereinafter.

***Sports***

In **Italy** biometrics, including a biometric database, are being used for access to sports centres. The Italian DPA encounters difficulties regarding the proportionality principle and the purpose limitation principle. It recently found that the processing of biometric data to regulate access to a sports centre was disproportionate.

***School***

In **Hungary** camera surveillance and biometric entry control systems[101] are being used in schools. The DPA of **Ireland** published on its website guidance notes regarding 'Biometrics in Schools, Colleges and other Educational Institutions'. In **Italy** biometrics, including a biometric database, are being used for access to schools.[102] The DPA of **Lithuania** encountered questions regarding the possibility to deploy in schools biometric systems using fingerprints. The Lithuanian DPA issued a prohibition order to use such systems.

***Workplace***

In **Estonia** the private sector makes use of fingerprints and iris scans for security and workplace entry reasons. In **Ireland** the principal difficulty across both the public and private sector arises from attempts to introduce biometric systems without consultation with and consent of intended users, such as employees in the workplace. The Irish DPA published guidance notes on its website regarding biometrics in the workplace. Also in **Italy** biometrics systems, including biometric databases, have been deployed in the workplace, in particular for the control of employees' access to workplace areas. The Italian DPA issued several decisions regarding the use of biometrics in the workplace: (1) the blanket, unrestricted use of biometric data is not permitted. On account of their nature, these data require specific precautions to prevent harming data subjects. Therefore, as a rule it is not permitted to process fingerprint data to control the number of hours worked by the employees; (2) using biometric data may only be justified in specific cases by taking account of the relevant purposes and context in which data are to be processed. This is the case, for example, if access to "sensitive areas" is to be regulated through the use of biometrics; (3) biometric verification and identification systems based on the reading of fingerprints stored as encrypted templates on media that are held exclusively by the relevant data subject should be preferred over centralised processing of biometric data. The DPA of **Malta** issued a paper entitled 'The Use of Biometrics Devices at the Workplace'. The DPA of **Monaco** prohibits the use of biometric systems based on fingerprints in the workplace. The private sector in **Serbia** makes use of biometric systems in the workplace to monitor the number of

[101] The Hungarian response does not specify what kind of biometrics is being used.
[102] The Italian response does not specify what kind of biometrics is being used.

hours worked by the employees. Due to the violation of data protection legislation the further processing of biometric data was prohibited.[103]

The country responses show that the main difficulties of using biometrics are being encountered in the contexts of sports, school and workplace. The DPA in **Italy** encounters problems concerning the proportionality principle and the purpose limitation principle and recently found that the processing of biometric data to regulate access to a sports centre was disproportionate. While biometric systems are deployed in schools in **Hungary** and **Italy**, the DPA of **Lithuania** issued a prohibition order to use biometric systems based on fingerprints in schools. Biometric systems are deployed in the workplace (in the private sector) in the following Member States: **Estonia**, **Ireland**, **Italy**, and **Serbia**. The Italian DPA issued several decisions containing the requirements for using biometrics in the workplace. **Monaco** prohibits the use of biometric systems based on fingerprints in the workplace.

[103] The Serbian response is not clear as to whether the processing of biometric data in the workplace had been prohibited at all, or only the *further* processing of biometric data for other purposes than initially intended, which is a significant difference.

# 8 Conclusions and recommendations

The overview of country reports shows that the recommendations made by the Council of Europe in the past (the Council of Europe's 2005 progress report and the Parliamentary Assembly's 2011 report) have not lost their relevance. A coherent legal framework on biometrics is still lacking at either the level of the Council of Europe, the European Union and the Member States. A small step forward is the relevant provisions on biometrics in the modernised convention 108 and the proposed EU regulation. The authors conclude and recommend (in bold) the following:

1. **In the opinion of the authors the 2011 Parliamentary Assembly's report on biometrics captures all the main issues of the current legal debate on biometrics. The report contains many creative policy ideas regarding the regulation of biometrics. The central message is that additional regulatory measures, either soft law or hard law, are needed to be implemented in order to keep pace with developments in biometric technology and to harmonise the biometric legal framework across the CoE Member States. Data protection legislation should for example include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data.**
2. The 2005 progress report of the Council of Europe's Consultative Committee and the Parliamentary Assembly's report of 2011 both recommend the use of templates instead of raw biometric data. Unfortunately, the country reports show that only Estonia and Italy have noticed and implemented this recommendation. **Regulatory initiatives should also include a correct and useful definition of 'biometric data'.** The country responses show that very few countries have adopted legislation specifically aimed at the protection of biometric data. Georgia and Montenegro are the only two countries which have adopted a definition of biometric data. France and Georgia are pioneering the field of data protection in general and biometric data in particular.
3. In the 2012 modernisation proposal of Convention 108, drafted by the Council of Europe's Consultative Committee of Convention 108, the new Article 6 on the processing of sensitive data includes a provision concerning biometrics. By means of this proposal the Committee categorizes biometric data as sensitive personal data. The 2013 draft explanatory report of the Consultative Committee includes the same categorisation, although it is not clear what the consequences of such a categorization are. **More reflection is warranted about defining biometric data as sensitive personal data as it may imply that no longer a distinction can be made between more and less intrusive types of biometric processing.** In the Marper judgment the European Court of Human Rights states that not all biometric data should be treated the same, because not all types of biometric data are equally intrusive. This strengthens the idea that research has to be conducted on the consequences of biometric data as a specific category of sensitive personal data prior to the introduction of a new article 6 in Convention 108. Dutch research on biometrics has been conducted by the Dutch independent foundation Privacy First which recently presented its 2012 annual report (see section 7.1.15). Privacy First's aim is to preserve and promote the right to privacy and a free society with a central focus on biometrics. Its 2012 annual report shows the issues Privacy First is concerned about, such as privacy issues about biometrics regarding the Dutch Passport Act and the access to centralised and decentralised fingerprint databases by Dutch and foreign secret services.
4. The European Court of Human Rights noted in its Marper judgment that "[…] all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of [Convention 108] as they relate to identified or identifiable individuals." Therefore, all biometric data allowing the identification of an individual is protected by Article 8 of the European Convention on Human Rights (ECHR), according to the Court. The Court, however, recognized in its Marper judgment that fingerprints need to be distinguished from cellular samples and DNA profiles. The Court

states that because of the information they contain, the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints. **In the Court's judgment one can find an argument not to label all biometric data as sensitive personal data. It is not clear what the consequences of such a categorization are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that no longer a distinction can be made between more and less intrusive types of biometric processing.** The Court also considers that States which claim to be a pioneer in the development of new technologies bear special responsibility for striking the right balance between biometric data retention and the right to respect for private life. **In the opinion of the authors of this report it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a privacy impact assessment. Such an obligation is provided in the proposed regulation, but it is not mentioned in the proposed directive.**

5. The European Commission, unlike the Council of Europe, does not define biometric data as sensitive personal data or even a special category of personal data. The Council of Europe steers another course. In the modernisation proposal of the Consultative Committee regarding Convention 108 and the Consultative Committee's 2013 draft explanatory report of the modernized version of Convention 108 biometric data is considered sensitive data. **The European Commission and the Council of Europe's Consultative Committee both acknowledge the importance of a standardised definition of biometric data as they both suggest one. The authors of this report endorse this acknowledgment.** The Committee's 2013 draft explanatory report contains the following definition of biometric data: "data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter". The European Commission and the Council of Europe are aware of the necessity to implement the requirement of a privacy impact assessment (sometimes called a data protection impact assessment). The Proposed Regulation contains such a requirement in Article 33, and the 2012 Modernisation Proposal of the Council of Europe's Consultative Committee includes such a requirement in Article 8bis(2). The country reports show that no Member State has yet implemented in their data protection legislation an obligation to perform a privacy impact assessment. However, France, Italy, Macedonia, Monaco, Montenegro and Slovenia incorporated the requirement of prior checking in their data protection legislation.
6. The Eurodac system, operational since 15 January 2003, enables European Union (EU) countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union. The 2006 Commission Staff Working Document of the Commission of the European Communities shows that in 2005 the EURODAC Central unit has again given very satisfactory results in terms of speed, output, security and cost-effectiveness. The Eurodac system has also attracted considerable criticism because it requires the mandatory disclosure of biometric information by people who have not committed a crime. The following data are registered: the Member State of origin, the digital fingerprint, the sex and the reference number used by the Member State of origin. **The registration of biometric data and other additional information of the data subject may pose risks such as function creep, particularly because the disclosure of biometric data is mandatory.**
7. The Schengen Information System (SIS) is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics (e.g. photos, fingerprints and, if necessary, even DNA profiles), the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. As soon as SIS II becomes operational it will increasingly be police crime investigation units who are interested in the SIS. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities.

The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. **The use of (biometric) data for another purpose than originally collected for, which is called function creep, poses serious risks for the individual's rights and freedoms, particularly if more authorities will be granted access to SIS.**

8. The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. The VIS database will include information about personal identification of visa applicants (including biometrical data such as facial image and fingerprints), status of visa, authority that issued the visa, and record of persons liable to pay board and lodging costs. **Because the disclosure of biometric data and other additional information is mandatory its registration may pose risks such as function creep.**
9. The Council of European Justice and Home Affairs ministers adopted Regulation (EC) No 2252/2004 ('Regulation on standards for security features and biometrics in passports and travel documents issued by Member States') on 13 December 2004 without taking into account proposed amendments of the European Parliament. Unlike Eurodac, SIS and VIS, the European biometric passport is applicable to all European citizens. Biometric systems used in the context of the European biometric passport therefore pose risks to the rights and freedoms of all European citizens. The choice for mandatory facial images as well as finger scans and the idea of a centralized database was not questioned. Furthermore, little attention has been paid by the EU institutions to publicly account for meeting the requirements of proportionality and necessity. **It can be concluded that the EU does not always pay adequate attention to privacy issues regarding biometrics. The country reports show that only few countries incorporate privacy protecting provisions in legislation concerning biometrics. Regulation on biometrics should not be left to Member States. The EU and the Council of Europe their selves should propose regulation.**
10. Second generation biometrics aims to identify a person on the basis of his or her actual behaviour or activities. Second generation biometrics comprises a new type of biometric features such as gait (manner of walking), voice, body odour, ECG (brainwave pattern), EEG (electrical activity of the heart), body temperature, and pupil dilation. These biometric characteristics can sometimes be collected from a distance whilst the data subject is unaware. This makes it more difficult to monitor whether biometric controllers comply with data protection legislation (e.g. informed consent by the data subject prior to biometric data processing). Due to second generation biometrics an incremental change from visible to invisible data collection may occur. Biometric data may be originally collected for one specific purpose, but subsequently used for another purpose (function creep). It becomes more difficult to exercise the right to object to certain types of data processing. Moreover, biometric data may be used for profiling activities, while it is not clear whether and when profiling falls directly under the Convention. The Council of Europe concludes in its 2010 Recommendation that it is necessary to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Second generation biometrics can be used for profiling, meaning that individuals can be categorized. Unjustified selection due to profiling may result in discrimination and stigmatisation. **In the opinion of the authors the debate about the future legal framework on data protection should include a discussion about the concerns regarding second generation biometrics, such as function creep, profiling, discrimination, and stigmatisation.**
11. All biometric systems (without exception) have some intrinsic errors having a negative effect on the system's performance and accuracy (i.e. efficacy). The main error rates are the failure to enrol (FTE), failure to acquire (FTA), false accept error (FAR) and false reject error (FRR). All four intrinsic errors negatively affect the efficacy and efficiency of a biometric system. The FTE can often be reduced by means of assistance of trained personnel (human intervention) to the individuals who need to provide their biometric. The FAR and FRR can be reduced (although not to zero) by increasing the quality of biometric images. The FTA furthermore (but also the FTE, FAR and FRR) can be reduced by employing multimodal biometric systems, which make use of several biometric modalities. Two design modes offer best accuracy: (1) multiple biometrics from

the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger). It can be concluded that the biometric systems' performance and accuracy depend on error rates, which can for example be reduced by human intervention, multimodal biometric systems and higher quality of biometric images. **The European legal framework on data protection should include provisions aiming to reduce the errors of biometric systems such as provisions on human intervention, multimodal biometrics, high quality images and fall-back procedures. In case of errors, alternative methods of identification and verification should be offered (see also the 2011 Parliamentary Assembly report).**

12. Biometric systems are susceptible to several threats, such as impostor threats (e.g. identity fraud, biometric database attack, enrolment fraud, spoofing and Trojan horse attacks) and additional threats (e.g. function creep, tracking and tracing, linking of biometric data to other personal information, system failures and leakage of biometric data). Several mechanisms to overcome vulnerabilities in biometric systems are human intervention, human supervision, liveness detection and multimodal biometrics. A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorized in feature transformation and the employment of a biometric cryptosystem. Both are effective methods to protect biometric templates. Although biometric templates as such are significantly more safely compared to the use of raw biometric data, the country reports show that very few countries address the need to use templates. The Council of Europe's 2005 progress report and the 2011 Parliamentary Assembly's both recommend the use of templates instead of raw biometric data, but Mr Haibach's recommendations (in the 2011 report) regarding the use of templates have been noticed only in Estonia and Italy. The Estonian report underlines the importance to use biometric templates instead of raw biometric data. The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects. For example, the storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases. **In the opinion of the authors data protection legislation should include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.**
13. 8 out of 22 Member States which responded to our questionnaire have adopted legislation specifically aimed at the protection of biometric data. These countries are: Estonia, France, Georgia, Italy, Macedonia, Monaco, Montenegro, and Slovenia. The provision included most often in data protection legislation of these Member States concerns prior checking. Prior checking is contained in data protection legislation of the following Member States: France, Italy, Macedonia, Monaco, Montenegro, and Slovenia. The Member States addressing biometric data as a special category of personal data are: Georgia and Macedonia. In Estonia biometric data is considered sensitive personal data. The Member States which adopted a definition of biometric data are: Georgia and Montenegro. Currently, neither Convention 108 nor the applicable European legislation specifically address biometrics. Provisions on prior checking have been adopted by several Member States, but are not (yet) addressed in legislation of the Council of Europe or the European Union.
14. The country responses show that the main difficulties of using biometrics are being encountered in the contexts of sports, school and workplace. The DPA in Italy encounters problems concerning the proportionality principle and the purpose limitation principle and recently found that the processing of biometric data to regulate access to a sports centre was disproportionate. While biometric systems are deployed in schools in Hungary and Italy, the DPA of Lithuania issued a prohibition order to use biometric systems based on fingerprints in schools. Biometric systems are deployed in the workplace (in the private sector) in the following Member States: Estonia, Ireland, Italy, and Serbia. The Italian DPA issued several decisions containing the

requirements for using biometrics in the workplace. Monaco prohibits the use of biometric systems based on fingerprints in the workplace. **Both the Council of Europe and the EU should propose soft law to regulate the legal issues in the contexts of sports, school and workplace.**

# Annex A: The recommendations in the 2005 progress report

The Council of Europe's 2005 progress report contains 12 recommendations:

**Recommendation 1:** 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.
**Recommendation 2:** 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.
**Recommendation 3:** 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.
**Recommendation 4:** 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.
**Recommendation 5:** 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.
**Recommendation 6:** 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.
**Recommendation 7:** 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.
**Recommendation 8:** 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.
**Recommendation 9:** 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.
**Recommendation 10:** 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.
**Recommendation 11:** 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.
**Recommendation 12:** 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.