



COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

ICT Policy Support Programme (ICT PSP)

ICT-PSP-2-Theme-3 - Consensus building, experience sharing
on internet evolution and security

ICT PSP call identifier: ICT PSP 2nd call for proposals 2008
ICT PSP Theme/objective identifier: 3.2 Trusted information infrastructures and
biometric technologies

Project acronym: BEST Network
Project full title: Biometrics European Stakeholder Network
Grant agreement no.: 238955

Deliverable D7.2

Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation

**Prepared by Paul de Hert and Annemarie Sprokkereef
(TILT, University of Tilburg)
With contributions from
Ann Cavoukian, Juliet Lodge, Thomas Probst and Max Snijder**

Classification: xx
Dissemination level: PU
Date of submission: November 2010

Table of Contents

Biometrics in Europe: Inventory on Biometric Data and Privacy legislation

1.	Introduction	
2.	The Background: International Sources of Data Protection	
3.	Strengths of European Data Protection	
3.1	Supervisory Authorities on Data Protection	
3.2	Biometrics and Data Protection	
3.3.	The Utility of European Data Protection	
3.4	European Data Protection as an Enabling Logic	
3.5	Security of Biometric Data	
4	EU Practice and Biometrics	
4.1	EURODAC	
4.2	The Schengen Information System (SIS)	
4.3	The Visa Information System (VIS)	
4.4	The European Biometric Passport	
5	National Developments	
5.1	Germany	
5.1.1.	Introduction	
5.1.2	Current Biometric Government Applications	
5.1.3	Legislation	
5.1.4	Data Protection Authorities and Biometrics	
5.2	United Kingdom.....	
5.2.1	Introduction	
5.2.2	Current Biometric Government Applications	
5.2.3	Legislation	
5.2.4	Data Protection Authority and Biometrics	
5.3	The Netherlands	
5.3.1	Introduction	

- 5.3.2 Current Biometric Government Applications
- 5.3.3 Legislation
- 5.3.4 Data Protection Authorities and Biometrics
- 6 Shortcomings of European Data Protection.....
 - 6.1 Enabling Without Limits.....
 - 6.2 'Secondary use' & 'Proportionality' vs. Diffusion Effect
 - 6.3 Second Generation Biometric Data: From Visible to Invisible Data Collection.....
- 7 Recommendations
- 8. Recent Materials for Further Reading

1. Introduction

In the 1970s, many European states passed data protection legislation. The objective of this legislation was to protect individuals against any negative or undesired effects resulting from the processing (i.e., the collection, use, storage, etc.) of personal data by public administrations and private actors. In general, these laws specify a series of rights for individuals and demand good data management practice on the part of the entities that process data ('data controllers').

The starting point of data protection was thus the desire to protect the citizen. The purpose became therefore to ensure that personal data are processed in ways that make it unlikely that personal integrity and privacy will be infringed or invaded. It is impossible to capture the essence of data protection in two or three lines here. It suffices to summarize that data protection is a *catch all* term for a series of ideas with regard to the processing of personal data. Through the application of these ideas legislators try to reconcile fundamental but conflicting values such as privacy and freedom of information, governmental need for surveillance and taxing, and so forth. In general, data protection does not have the prohibitive nature of criminal law. Data subjects do not own their data and can often not prevent processing of their data. Under the current state of affairs, data controllers have a right to process data pertaining to others. Hence, data protection is pragmatic of nature: it assumes that private and public actors need to be able to use personal information and that this must be accepted in the normal course of events.

2. The Background: International Sources of Data Protection

The basic practices or principles of data protection are spelled out in the international legal data protection texts produced by institutions such as the Organisation for Economic Co-operation and Development (OECD),¹ the Council of Europe², the UN³ and the European Union.⁴ Each of these organisations produced what have become classic

¹ OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317.

² Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, no. 108; *International Legal Materials*, 1981, I, 422

³ The *United Nations Guidelines concerning computerized personal data files*, adopted by the General Assembly on 14 December 1990.

⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal of the European Communities*, L 281, 23 November 1995, 31-50.

data protection instruments, respectively the OECD Guidelines, the Treaty 108 and the Data Protection Directive.⁵ The EU has also included the right to data protection in the European Charter of Fundamental Rights.⁶ The European data protection framework applies to all personal data without exception.⁷ It applies not only to the public sector, but also to the private sector and to legal conflicts between citizens. Special watchdogs such as the European or National Data Supervisors have been created and positioned next to the judiciary. One of their tasks is to identify new threats to rights and liberties created by the use of new technologies such as biometrics.

The OECD Guidelines take the form of a short document that contains no more than a listing of the data protection principles.⁸ These principles are: 1. the collection limitation principle;⁹ 2. the data quality principle;¹⁰ 3. the purpose specification principle;¹¹ 4. the use limitation principle;¹² 5. the security safeguards principle;¹³ 6. the openness principle;¹⁴ 7. the individual participation principle;¹⁵ 8. the accountability principle¹⁶. These principles apply to all personal data handled in the public or private domain.

The national sources of data protection are diverse but all provide for a series of rights for individuals such as the right to receive certain information whenever data are collected, the right of access to the data, and if necessary, the right to have the data corrected, and the right to object to certain types of data processing. Also, these laws generally demand good data management practices on the part of the data controllers

⁵ This Directive has been supplemented by data protection provisions in a number of more specific directives .

⁶ Charter of Fundamental Rights of 7 December 2000 of the European Union, *Official Journal of the European Communities*, C 364, 2000, 1, entered into force December 7, 2000.

⁷ Of course apart from the exceptions in the context of law enforcement, state security and so forth.

⁸ The two European instruments widen the scope in many respects and create supervisory data protection committees, which are unknown in the context of the OECD Guidelines.

⁹ There should be limits to the collection of personal data and any such information should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

¹⁰ Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and up-to-date.

¹¹ The purposes for which personal data are collected should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

¹² Personal data should not be disclosed, made available or otherwise used for purposes other than those first specified except: a) with the consent of the data subject; or b) by the authority of the law.

¹³ Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

¹⁴ There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

¹⁵ An individual should have the right of notification, access and rectification.

¹⁶ A data controller should be accountable for complying with measures that give effect to the data protection principles.

and include a series of obligations: the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to guarantee the security of the data against accidental or unauthorized access or manipulation, and in some cases the obligation to notify a specific independent supervisory body before carrying out certain types of data processing operations. These laws normally provide specific safeguards or special procedures to be applied in case of transfers of data abroad.

3. Strengths of European Data Protection

The EU data protection framework is governed by three instruments: a general Directive 95/46/EC¹⁷, a specific Directive 97/66/EC¹⁸ concerning the processing of personal data and the protection of privacy in the telecommunications sector (replaced by the privacy and electronic communications Directive 2002/58/EC in 31 October 2003)¹⁹ and Regulation (CE) No 45/2001 of the European Parliament and of the Council of 18 December 2001, on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.²⁰

The general Directive applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. It does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and to processing of personal data in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defense or State security.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down rights for the person whose data is processed and guidelines and duties for the controller,²¹ or processor²² determining

¹⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal*, L 281, 23 November 1995, 31-50, hereinafter: "the Directive".

¹⁸ Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and protection of privacy in the telecommunications sector; *Official Journal*, L 024 , 30 January 1998, 1-8

¹⁹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and protection of privacy in the electronic communications sector, *Official Journal* L 201, 31 July 2002. Article 3 §1 states: "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community".

²⁰ *Official Journal*, L 8, 12 January 2001

²¹ Directive 95/46/EC, Article 2(d): "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data where the purposes and means of processing are determined by national or

when this processing is lawful. The rights, duties and guidelines relate to: data quality; making data processing legitimate; special categories of processing; information to be given to the data subject; the data subject's right of access to data; the data subject's right to object to data processing; confidentiality and security of processing; notification of processing to a supervisory authority.

Central notion in the Directive is *personal data*, meaning any information relating to an identified or identifiable individual (*infra*). Data protection does not focus specifically on the instruments used for the surveillance of for the processing, but only looks at the object of these actions, namely human data. Regardless of specific technologies that are being used, whenever there is processing of personal data, the data protection principles apply.

The biggest breakthrough relates to the scope of the Directive. The Directive brings electronic visual and auditive processing systems explicitly under its scope. The preamble says "*Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques uses to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data*".²³

Processing of sound and visual data is thus considered as an action on which the Directive is applicable. *Processing* is very broad: it can be automatic or manual and can consist of one of the following operations: collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission and so forth. The sheer fact of collecting visual (for example face scan) or sound data can be considered as *processing*.

The Directive contains a detailed set of rules for transfers of personal data from a Member State to a third country. These transfers are authorized when the country in question has an 'adequate level of protection'. However, they may not be made to a third country, which does not ensure this level of protection, except in the cases of the derogation listed.

Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

²² Directive 95/46/EC, Article 2(e): " 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

²³ Directive 95/46/EC, Preamble, § 14.

3.1 Supervisory Authorities on Data Protection

The Directive also introduced a duty to set up data protection authorities in all Member States.²⁴ These supervisory authorities are intended as watchdogs endowed with investigative and regulatory powers.

Data protection authorities must act in complete independence when exercising the functions entrusted to them. They are competent to hear claims on data protection lodged by any person or by an association representing that person.

They are endowed with investigative powers, such as powers of access to data, forming the subject matter of processing operations and powers to collect all the information necessary for the performance of their supervisory duties.

They are also endowed with effective powers of intervention, such as, delivering opinions before processing operations are carried out, and ensuring appropriate publication of such opinions, ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, of warning or admonishing the controller, and referring the matter to national parliaments or other political institutions.

Article 28³ of the Directive gives them the crucial power of *a prior consent*. Without this consent processing of personal data by governmental bodies or by individuals is not allowed and the European supervisory bodies must check processing proposals before they consent. Following this prior check, the body, may give an opinion or (depending on national law) an authorization regarding the processing.

Also they have the power to engage in legal proceedings or to bring violations to the attention of the judicial authorities, where the national provisions adopted pursuant to Directive 95/46/EC have been violated.²⁵ Note that the Directive does not impose the use of criminal sanctions for violations of the principles on Member States, but most data protection laws do contain criminal sanctions. Decisions by the supervisory authority, which give rise to complaints, may be appealed against through the courts. Furthermore, those supervisory authorities have the obligation to draw up a regular report on their activities and may also be requested to exercise its powers by an authority of another Member State.

²⁴ Directive 95/46/EC, Article 28¹: "Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them".

²⁵ Directive 95/46/EC, Article 28³

3.2. Biometrics and Data Protection

“Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics”.²⁶ Although the term 'biometrics' does not appear in the Directive, it is seemingly indisputable that their processing involves 'capturing, transmitting, manipulating, recording, storing or communicating sound and image data relating to natural persons' in the sense of the Directive. Hence, the Directive applies to processing involving such data.

The Directive equates 'personal data' with any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.²⁷ Raw biometrical images of a person are personal data in the sense of the Directive. The Directive is also applicable to the templates derived from raw biometrical images. This kind of data should be seen as indexical data, no different from e.g. a written report on a person when processed in a personal computer.

It is sufficient for the Directive that data make it possible to identify a person, it is not necessary to know the name of the person to speak of 'personal data' in the sense of the Directive. At the same time, this interpretation, including any revocability criteria, has never been tested in a court of law.

Although not all biometrical data is sensitive in common knowledge terms or in data protection terms, they are collected and stored in order to identify persons. The Directive does not apply to anonymous data, but it draws a very high line for this. The notion of 'identifiable' in the European Directive is, unlike other legal international data protection texts, very extensive. Data that at first glance does not 'look' like personal data can very often be led back to an individual. It is not because a processor *wants* data to be anonymous, that data *is regarded* as anonymous.²⁸ The definition of 'identifiable' is so broad that data can be considered personal as long as the controller himself is still able to identify the persons behind the data.²⁹

All biometrical technologies are covered by the Directive, with or without recording of the 'raw image' or with or without use of templates. With a small but important exception for police and justice (infra), the Directive covers their use by public bodies

²⁶ ISO SC37 Harmonized Biometric Vocabulary.

²⁷ Directive 95/46/EC, Article 2(a).

²⁸ Blas (2003) 503: gives the example of a proposed large-scale database in Iceland. This envisaged database was supposed to contain anonymous data. However in a small country genetic information is likely to indicate biological lineage and to reveal identities of persons concerned. The security measures initially proposed by Iceland to replace identifiers by a code were therefore not sufficient to guarantee the anonymity of the Icelandic population.

²⁹ Too often controllers assume they are processing anonymous data when an average individual other than themselves are unable to determine the name of the persons.

and private bodies. The following applies some of the sometimes very specific data protection principles of the Directive to the subject matter: biometrics.³⁰

- a.* biometrical information must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (art. 6°1b);
- b.* before processing any biometrical information the supervisory body has to be notified of the purposes of the processing (art. 18);
- c.* biometrics should be collected and processed fairly and lawfully; the processing of biometrical data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and the processing of data concerning health or sex life should be prohibited as a rule (art. 8);
- d.* the collection and processing must be adequate, relevant and not excessive in relation to the declared purposes (art. 6°1c);
- e.* biometrical images have to be accurate and, where necessary, kept up to date or erased (art. 6°1d);
- f.* biometrical data may not be disclosed to third persons if this doesn't follow out of the declared purpose (art. 17 and 19);
- g.* the biometrical data subject has a right to know about the processing and the use of the processed biometrics (art. 10-11);
- h.* all biometrical data subjects are endowed with a right of access to the biometrical data and to obtain rectification, erasure or blocking of data when the processing violates the provisions (e.g. incomplete or inaccurate nature of the data). In some cases these rights are restricted to safeguard national security, defence, public security, prevention and criminal investigation, economic or financial interests of states, rights and freedoms of others (art. 13);
- i.* every biometrical data subject has a right not to be subject to a decision which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, credit-worthiness, reliability, conduct, etc (art. 15);
- j.* there has to be a responsible controller³¹ to ensure data protection rights and duties (art. 6°2-16, 17, 18, 19).

3.3 The Utility of European Data Protection

The practical utility of the European data protection framework is evident. Rights for those who are controlled and verified, duties and control for those who install biometrical technology, and process biometrical data regardless of the location, be it in

³⁰ It was already made clear above that the word biometric does not feature in the Directive and these provisions are an interpretation. Compare with De Hert, 1997.

³¹ "Controller shall mean the natural or legal person, public authority, agency or any body which alone or jointly with others determines the purposes and means of the processing of personal data (...)" (art. 2d).

an open field or a private house, and regardless of the capacity of the processor (citizen or government official).³² The framework has a general scope and applies to all existing biometric technologies: fingerprints, iris scans, face recognition, DNA³³, etc. The 'disruptive novelty' of contemporary use of biometrics, the use of technology, is taken into account by a broad definition of the term 'processing'. *The complex question "is this a privacy issue?" is replaced by a more neutral and objective question "are personal data processed?"* Data protection, as such, is a general framework for all kinds of surveillance: the written word, sounds, images, DNA and even smells can create personal data in the meaning of the directive.

There is furthermore little or no room for secret biometrical surveillance by private persons since there is a duty to inform the data subject.³⁴ An antisocial or even racist use of biometrical data is considered a violation of article 15 (right not to be subject to a decision which is based solely on automated processing of data intended to evaluate certain personal aspects (work, credit-worthiness, reliability, conduct, etc)).³⁵

The rules for exchange of data with third countries allow for 'biometrical co-operation' under controlled conditions. Article 25 of the European Directive imposes an obligation on member States to ensure that any personal information relating to European citizens is protected by law when it is exported to and processed in, countries outside Europe.³⁶ Countries that refuse to adopt meaningful privacy laws³⁷ may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data such as biometrical data.

3.4 European Data Protection as an Enabling Logic

Data protection has grown in response to problems generated by new technology. It

³² Some data protection rights of the data subjects can be restricted to safeguard e.g. national security, defence, public security, prevention and criminal investigation.

³³ Technically, DNA is not a biometric since it is not automated (see also section 5.2.2. below).

Nevertheless, it is often considered a biometric due to its strength in identifying individuals.

³⁴ Exceptions to the duty to inform the subject are provided for on behalf of law enforcement and intelligence authorities, although these do not fall under the Directive.

³⁵ Directive 95/46/EC, Article 15.1.: "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc".

³⁶ Article 25 states: "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection".

³⁷ An assessment of a third country's privacy protection system is made by the European Commission. The overarching principle in this determination process is that the level of protection in the receiving country must be "adequate" rather than "equivalent." Therefore, a reasonably high standard of protection is expected from the third party, although the precise dictates of the Directive need not be followed.

brings no added value to reduce all these responses to “privacy” only. Other values and concerns are also at play, for example, the right not to be discriminated against protected by Article 15 of the Data Protection Directive. According to this provision every person has the right “not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data.” The provision refers to automated processing of data “intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.” The goal is to guarantee everyone's participation in important personal decisions. A dismissal based purely on the data from the company time clock is, as a result, unacceptable. It applies also to the rejection of a job seeker based on the results of a computerized psycho-technical assessment test or to a computerized job application package. Those decisions have to take professional experience or the result of a job interview into account. The automated test is insufficient and it applies to such sectors as banking and insurance. EU member states have to enact provisions that allow for the legal challenge of computerized decisions and which guarantee an individual's input in the decision-making procedures.³⁸

Last but not least is the principled stand of data protection towards technology. Data protection is characterized by an 'enabling logic'. It makes existing processing practices transparent, but as a rule does not prohibit them.³⁹ Data protection regulations create a legal framework based upon the assumption that the processing of personal data is allowed and legal in principle.⁴⁰ Therefore data protection regulations do not recognize ownership of the individual regarding his data, but only grants the individual controlling rights. As a matter of fact data protection does not recognize any ownership rights at all. Neither the individuals, nor collector for his intellectual contribution or the institution where data are collected, are property rights holders with regard to the data. There is also no question of shared ownership. There is simply no ownership. Data flows, it belongs to everybody. Concerns with regard to privacy, data protection *and* intellectual property rights may lead to certain regulations that aim at distributing certain procedural rights and patrimonial rights, but their reach remains within strict limits far away from all suggestions of a property right.

³⁸ However member states are allowed to grant exemptions on the ban on computerized individual decisions if such a decision "(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

³⁹ There are exceptions: parts of the data protection regime that provide for a prohibition of processing (e.g. sensitive data, secretly collected personal data) actually fall under a privacy or opacity ruling.

⁴⁰ An outright processing ban effectively applies only to special categories of sensitive personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

3.5 Security of Biometric Data

Articles 16 and 17 of the Directive require certain security obligations from the controller and the processor.⁴¹ The notion of processing in the Directive refers not only to the moment a computer is processing personal data, but instead relates to a much wider activity. For those that process biometrical data this means that the duty to implement security measures should be respected not only at the moment data are collected, but also at later stages when data are stored or disclosed.

Article 17 of the Directive reads as an open invitation to the European legislator to supplement the Directive with additional measures with regard to biometrics. Although national data protection legislation sometimes contains criminal sanctions for the controller disrespecting some of the duties of the Directive, no country has made inadequate protection of personal data a crime.

Prins has rightly held that having in mind the nature of biometric information it appears that a high level of security is likely to be required to meet conditions set by the law.⁴² She raised the question whether certain (smaller) organizations are in a position to maintain the required (high) level of protection where they keep biometric information or original scanned images in databases. "Security considerations could thus restrict the use of biometric technologies as far as on-line databases used by small organizations is concerned".⁴³ Prins added: "This brings us to the issue of the management and protection of (large) databases containing biometric information. Ultimately, this requires the attention of policy makers for society cannot end up with numerous warehouses containing biometric information that may all be easily connected to other personal information or data warehouses".⁴⁴ In a recent case study on the use of biometrics in semi public organizations in the Netherlands, several protection breaches were found that confirm that small organizations in the Netherlands have difficulties keeping up with data protection requirements when storing the data collected on data bases in their organization.⁴⁵

Security can be an argument against certain biometrical applications, but because of the nature of biometrics, it may not come as a surprise that the issue of security can also be

⁴¹ In particular Directive 95/46/EC, Article 17.1: "Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected".

⁴² Prins, 1998 *I.c.*, 162.

⁴³ Prins, 1998 *I.c.*, 162.

⁴⁴ Prins, 1998 *I.c.*, 162.

⁴⁵ De Hert and Sprokkereef, 2009.

looked at in favour of biometrics. The Directive demands an adequate level of safeguard, and a balance must be found between the interests to be protected, the technical possibilities and the cost of implementation of the measures. Applied to the use of biometric technology, Prins argues that for this moment, the demands posed on security are not stringent enough to *necessitate* this technology. She continues, however, saying that "it might very well be that with developments in both technology and fraudulent practices, the use of biometric technologies may become a condition of the qualification 'adequate' protection (e.g. social service benefits). If at some point in the future the quality of critical social processes is to be guaranteed, biometric technologies are required to determine the true identity of individuals. The use of biometric technology thus becomes a tool of public policy".⁴⁶

The foregoing shows, that the argument that biometric technologies are more reliable identification techniques can be turned into a privacy argument in favour of biometrics. The argument can also be grounded upon Article 6.1.(d) of the Directive: personal data must be accurate and, where necessary, kept up to date; "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified". Processors that chose for biometrical identification can on this basis defend their choice using privacy arguments. Of course the argument has nothing to do with privacy. Data protection regulations defend many different values and goods. Privacy is only one of them. Security duties in the European legal framework are rooted in privacy and personal data protection regulation, but serve different purposes. Regardless of this, the fact remains that duties to protect the security of personal data can be balanced against privacy concerns about well-performing identification systems. There is also the issue of biometrics as a privacy enhancing technology (PET). In the current state of the art biometric privacy enhancing technology can be used to enhance authorization processes. This way biometrics serves to protect data subjects whose data are stored within a system against unauthorized access by data controllers. Biometrics as PET can also act as an extra protection against unauthorized individuals from outside trying to hack into the system. The debate whether biometrics can be a PET when it is used for identification purposes, and storage on a data base is required, is still ongoing. In general, biometrics as a whole is not considered PET. There is indeed an argument that biometric-enabled access control may protect even more sensitive data, e.g. health records. However, the term PET is mostly reserved for "privacy by design" technologies called "untraceable biometrics" or "biometric encryption".⁴⁷

⁴⁶ Prins, 1998, *I.c.*, 162.

⁴⁷ A. Cavoukian and M. Snijder, "A Discussion of Biometrics for Authentication Purposes: The Relevance of Untraceable Biometrics and Biometric Encryption". See: <http://www.ipc.on.ca/images/Resources/untraceable-be.pdf>.

4 EU and Biometrics in Practice

4.1 EURODAC

The Eurodac system (Council Regulation of 11 December 2000⁴⁸) enables Member States to identify asylum-seekers and persons who have crossed an external frontier of the Community in an irregular manner. By comparing fingerprints Member States can determine whether an asylum-seeker or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State.

Eurodac consists of a Central Unit within the Commission equipped with a computerized central database for comparing the fingerprints of asylum applicants and a system for electronic data transmission between Member States and the database.⁴⁹ In addition to fingerprints, data sent by Member States will include in particular the Member State of origin, the place and date of the asylum application if applicable, sex and reference number.⁵⁰ Data are collected for anyone over 14 years of age and are encoded directly into the database by the Central Unit or the Member State of origin.⁵¹

In the case of asylum-seekers, data are kept for 10 years unless the individual obtains the citizenship of one of the Member States, when their particulars are immediately

⁴⁸ Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *Official Journal* L 316, 15.12.2000. Cf. "Eurodac" system, 10 April 2003, 3p. via

<http://europa.eu.int/scadplus/printversion/en/lvb/l33081.htm> The Dublin Convention of 15 June 1990, to which all Member States are party, provides a mechanism for determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Union. In view of the difficulties the Member States anticipated in identifying aliens who had already lodged an asylum application in another Member State, Ministers responsible for immigration agreed, in 1991, to establish a Community-wide system for the comparison of the fingerprints of asylum applicants.

⁴⁹ Council Regulation No 2725/2000, Article 1.2.

⁵⁰ Council Regulation No 2725/2000, Article 5.

⁵¹ See on this Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *Official Journal* L 62, 5 March 2002 and Commission communication regarding the implementation of Council Regulation (EC) No 2725/2000 "Eurodac", *Official Journal* C 5 of 10 January 2003. In accordance with Article 22 of the "Eurodac" Regulation, the Council adopted certain provisions for the transmission and comparison of fingerprints and the definition of the tasks of the central unit. The Central Unit defines the technical requirements for transmitting fingerprints electronically. In the event of technical problems, other means of transmission are possible (CD-ROM, diskettes, paper, etc.). A reference number makes it possible to relate a fingerprint to one particular person and to identify the Member State that sent the data. The number is composed of several letters and a code. Member States ensure the transmission of fingerprints in "an appropriate quality" for the purpose of comparison. As a general rule, the Central Unit deals with requests for comparisons within 24 hours (except in case of emergency), in order of arrival.

erased.⁵² Data relating to foreign nationals apprehended when attempting to cross an external border irregularly are kept for two years from the date on which the fingerprints were taken. Data are immediately erased before the end of the two years if: the foreign national receives a residence permit, or has left the territory of the Member States.

In the case of foreign nationals found illegally present within a Member State, Eurodac makes it possible to check their fingerprints against those in the central database to determine whether the individual had previously lodged an asylum application in another Member State. After the fingerprints have been transmitted for comparison purposes Eurodac does not store them.⁵³

Directive 95/46/EC applies to Eurodac, and the Regulation itself also contains a proper system of data protection. Member States of origin must ensure that fingerprints are taken lawfully as well as all operations involving the use, transmission, conservation or erasure of the data themselves. The Commission must see to the proper application of the Regulation within the Central Unit, and take the necessary measures to ensure the safety of the Central Unit. It also informs the European Parliament and the Council of the measures it takes. Any person or Member State that has suffered damage as a result of an unlawful processing operation or an act incompatible with the Regulation is entitled to receive compensation. That State may, however, be exempted from its liability, in whole or in part, if it can prove that it is not responsible for the event giving rise to the damage.⁵⁴

In addition to the national supervisory bodies, an independent joint supervisory authority is set up, consisting of a maximum of two representatives from the supervisory authorities of each Member State. The joint supervisory authority has the task of monitoring the activities of the Central Unit to ensure that the rights of data subjects are not violated and to resolve implementation problems in connection with the operation of Eurodac.⁵⁵ In July 2007 this Eurodac Supervision Coordination group⁵⁶ published its first coordinated inspection report.⁵⁷ The recommendations of the report focussed on special searches, use for other purposes and quality of fingerprints.

The rights of the data subject are in line with those specified by the Directive and include: that he or she must be informed of the purpose for processing the data within Eurodac, of the obligation to have the fingerprints taken, of the right to rectify data, and

⁵² Article 6 *juncto* 7 of Council Regulation No 2725/2000.

⁵³ Article 10 of Council Regulation No 2725/2000.

⁵⁴ Council Regulation No 2725/2000, Article 17.

⁵⁵ Council Regulation No 2725/2000, Article 20. Eventually, the joint supervisory authority will be replaced by the independent supervisory body under Article 286(2) of the EC Treaty. See on this Article 20.11.

⁵⁶ Composed of representatives from the Data protection Authority of each of the participating States and the European Data protection Supervisor.

⁵⁷ Can be obtained from the supervision secretariat: edps@edps.europa.eu.

finally, the right to request that factually inaccurate or unlawfully recorded data be corrected or erased (Arts 15 - 18). 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. Alterman⁵⁸ considers that Eurodac as a government database “is a clear case of taking the person as a mere thing, using their body as a means to an end”. There have been concerns whether the technical reliability of the biometric identification within Eurodac is of an appropriate standard. The so-called ‘False Rejection Rate’ of the various biometric identifiers is estimated between 0.5 and 1 %, although official figures vary and are subject to interpretation.⁵⁹ These arguments appear not to have had any impact on the decision making process related to Eurodac or on other European initiatives involving biometrics.

In summary, Eurodac is a computerized, central database which holds biometric fingerprint data on asylum seekers, aliens apprehended in connection with irregular border crossing, and aliens found illegally present in a Member State. In general, these data are held for 10 years unless the individuals obtain citizenship. The purpose of Eurodac is to help establish the responsible State, by recording the country an asylum seeker made his or her first asylum application, or the country he or she was previously resident. Eurodac is, therefore, a database designed to search for a so-called ‘hit’, which occurs when transmitted fingerprints match with the fingerprints already stored in Eurodac. Member States can then establish whether an asylum seeker has previously stayed in another Member State. The aim of the database is to determine which EU Member State is responsible for examining an application for asylum. The data are used for identification. A general unit carries out the comparisons; Member States themselves cannot conduct searches in data transmitted by other Member States. Biometric verification or identification is becoming an integral part of many new measures involving the need to identify individuals. The introduction of the biometric European passport (see below) means that mandatory disclosure of biometric information has been extended to all European citizens who want to travel outside the European Union.

⁵⁸ Altermann, 1996.

⁵⁹ See the paper by Brouwer that can be retrieved from the Challenge website, *Data Surveillance and Border Control in the EU*, <http://www.libertysecurity.org/article289.html>.

4.2 The Schengen Information System

The Schengen Information System (SIS) is an EU large scale computerized database, which has been operational since 1995. It was created as a compensatory measure following the abolition of controls at internal borders within the Schengen area, and was integrated into the EU framework by the Amsterdam Treaty. The objective of SIS I is to exchange data on people, including immigration data, and objects in order to uphold security, it does not contain biometric data. A Second Generation system SIS II was agreed by the EU Justice and Home Affairs Ministers on 2 June 2006 and has replaced SIS I.⁶⁰ 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.

The Schengen Information System is thus an information system that allows the competent authorities in the Member States to obtain information regarding certain categories of persons and property. The system is a mixed first and third pillar instrument, since it contributes to the implementation of the provisions on the free movement of persons (Title IV of the Treaty) and to judicial co-operation in criminal matters and police co-operation (Title VI of the Treaty).⁶¹ The idea behind the system is this of fast verification. As free movement within the Schengen area is only guaranteed to persons living legally in a Member State, reliable information systems are required in order to provide adequate and exchangeable information about nationals of third countries wishing to enter or live in the EU. The Schengen Information System therefore contains information about third country nationals who are to be refused entry to the Schengen Area, as well as data about wanted criminals and suspects (for extradition purposes), missing persons, and stolen and missing objects (vehicles, firearms, bank notes etc.). Its purpose is to allow checks on persons to be made quickly and efficiently at border controls in order to detect criminals and illegal immigrants moving into and

⁶⁰ OJ L 411/78 Council Decision 2006/1007/JHA of 21 December 2006 amending Decision 2001/886/JHA of the second generation Schengen system (SIS II). See also the Commission staff working document progress report January - December 2006 SEC (2007) 408 of 23rd March 2007 on the development of the second generation Schengen Information System (SIS II) and cover note 7829/07 from the Secretary-General of the European Commission available at <http://www.statewatch.org/news/2007/apr/eu-com-sis-sec-408.pdf>.

⁶¹ The purpose of the SIS is to improve police and judicial cooperation in criminal matters (covered by Title VI of the Treaty on European Union) and policy as regards visas, immigration and free movement of persons (covered by Title IV of the EC Treaty). The mixed nature of the SIS has been confirmed in the Council decision authorising the United Kingdom to participate partly in the SIS and in two Belgian-Swedish initiatives (a decision and a regulation) adopted by the Council on 6 December 2001 (*Official Journal* L 328, 13.12.2001).

from one Schengen country to another. The SIS is accessible to authorized persons within the police/border guards of Member States and also to some extent within embassies/immigration offices, with multiple queries and national interfaces.⁶²

The current SIS, grounded on the 1990 Schengen Convention,⁶³ was technically designed to cope with eighteen States (15 Member States, Iceland and Norway, and one in reserve). A new system -SIS II- is under its way to cope with the enlargement of the Union *and* to satisfy new police demands. Basically these demands deal with on new functions and new information types in the system and with the possibility of linking the system with other existing systems (see *below*, discussion of the VIS system). One of the demands regards the extension of storage times and therefore the increase in person specific data. Until now, there was a general three-year limit for the storage of personal data after which the inputting agencies had to check if the data was still necessary.⁶⁴ The SIS, which up to now had rather simple search/inquiring capacities, is to get expanded search powers in its second generation, for the "officer on the spot". In the case of cars, this means that the officers can enter parts of the chassis number as search criterion, if the number is not fully recognizable. In the case of personal identification papers, the first name as well as the date of issue will serve as search criteria.⁶⁵ 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

⁶² SIS currently consists of a national system located in each of the Contracting Parties (The Contracting Parties are countries (in the future, some can also be organisations: Europol for example). The systems data file has to remain materially identical to the national data file located in the national systems of each of the other Contracting Parties, by means of a technical support function. By virtue of Article 92 of the Schengen Convention, implementing the Schengen agreement of 14 June 1985, France is responsible for the technical support function located in Strasbourg in a custom-built, high security environment. The Strasbourg system is also called the C.SIS (i.e. the central part of the SIS). The support function comprises a central data file, which ensures, via on-line transmission, that the data files of the national systems contain identical information.

⁶³ The Schengen agreement was originally signed on 14 June 1985 by five EU countries (Belgium, the Netherlands, Luxembourg, France and Germany) to end border checkpoints and controls and harmonise external border controls, in order to promote free movement of persons in Europe. A Convention Implementing the Schengen Agreement was signed on 19 June 1990, laying down the measures designed to create, following the abolition of common border checks, a common area of security and justice. These measures include, among other things, the harmonisation of provisions relating to entry and short stays in the Schengen area by non-EU citizens (uniform Schengen visa) and asylum matters (determining in which Member State an application for asylum may be submitted).

⁶⁴ The only exception to this rule were alerts under Article 99 of the Schengen Convention: in cases of discreet surveillance, personal records could only be stored for up to one year. Critical about this demand, that can be compared to the chances made to British DNA regulations: 'Schengen Information System - SIS II: technical innovation a pretext for more data and more control' *Statewatch bulletin*, vol 11 no 1, Jan-Feb 2001, 2.

⁶⁵ 'Schengen Information System - SIS II: technical innovation a pretext for more data and more control' *Statewatch bulletin*, vol 11 no 1, Jan-Feb 2001

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.⁶⁶

The inclusion of biometrics is defended with reference to the growing difficulties of law enforcement authorities related to person identity checks and entry control, which can no longer be solved by a simple name search. The communication of the Commission illustrates this with three several examples,⁶⁷ and advances biometric identification or the query on biometric data as the appropriate solution for person identification.

In many EU Member States access to data held on SIS I has been a contentious issue. According to the Schengen Convention, data in SIS I can be searched and accessed by authorities designated by the contracting parties for the purpose of border checks and controls, and other police and customs checks, when carried out inside the country and in accordance with national law. Data relating to foreign nationals⁶⁸ may be searched by authorities responsible for issuing visas, residence permits or the administration of aliens. Schengen does not set limits to the number of persons with access authority, leaving access regulation to the national laws of the contracting parties instead. Consequently, the lists of people with access differ considerably from country to country. Access to SIS II will be widened to authorities such as vehicle licensing authorities, Europol, Eurojust and national prosecutors. SIS II, however, will only store biometric information that can be legally linked to an alert in SIS II.⁶⁹

Competent authorities will use SIS II to exchange data, including biometric fingerprints and face scans, using the same platform as VIS (see above) but with a

⁶⁶ *Ibid.*

⁶⁷ "-persons who know or assume they are stored in the SIS will try to hide their real identity by using false names (e.g. aliens subject to expulsion decisions). Even if the travel document produced is genuine, a SIS check using only a name search will fail.

-Assuming that a person has been apprehended using a false document, the real identity is unknown. With the current SIS functionality it is impossible to establish that the person is, for example, a wanted person and stored in the SIS under another identity.

-Multiple hits for a person with a common name (e.g. Schultze, Dupuis and basically any common family name) occur and make it very difficult to identify the person concerned. Citizens of countries with a traditionally more limited variety of family names (e.g. Bulgaria) might be particularly affected. This leads to potentially embarrassing situations for finally innocent persons and to ensuing operational and legal problems. A bilateral exchange of biometric data could be started now via the SIRENE offices. However the growing number of Schengen partners excludes, from a practical point of view, such multiple exchanges for those cases. In addition, the reliability of results would be doubtful" (Commission Communication to the European Parliament and the Council. 'Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)', COM(2003) 771 final - Brussels, 11 december 2003, 16).

⁶⁸ This concerns data entered pursuant to Article 96.

⁶⁹ For an overall view on the interoperability and synergies among European databases envisaged in the area of Justice and Home Affairs, see COM (2005) 597 final (Commission, 2005).

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.⁷⁰ 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. Despite these concerns about function creep and the use of a technology at such a large scale without substantial testing, SIS II can be regarded as a relatively benign system in terms of privacy.

4.3 The Visa Information System (VIS)

In order to create synergies, the SIS II runs on a common technical platform with the Visa Information System (VIS). The VIS project aims to develop and deploy a large-scale information system for visa requests to enter Schengen area countries. The system 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.⁷¹ 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 2001.⁷²

Both the SIS II and the VIS will consist of a central infrastructure and information system and of national interfaces providing the connection to relevant authorities in the

⁷⁰ See H.Dijstelbloem & A.Meijer (eds.) *Migration and the new technological borders of Europe*, (Palgrave MacMillan, forthcoming).

⁷¹ Commission Communication to the European Parliament and the Council. 'Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)', *I.c.*, 25-26.

⁷² 'European Commission awards contract for development of SIS II and VIS', *eGovernment News*, 28 October 2004, 2p. via <http://europa.eu.int/ida/en/document/3424>

respective Member States. Responsibility for updating or setting up the national parts of the SIS II and VIS will lie with the Member States. Despite running on a common architecture and platform, the VIS and SIS II will be two different systems with strictly separated data and access.

Biometric data (digital facial image and fingerprints) have been added to the VIS.⁷³ 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 Thessaloniki European Council on 19 and 20 June 2003 stressed that “a coherent approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonized solutions for documents for third country nationals, passports of Union citizens and information systems (VIS and SIS II).⁷⁴ The European Justice and Home Affairs Council held on 19 February 2004 adopted conclusions on the architecture, functionalities and biometric identifiers to be included in the future VIS, which will serve as a basis for the Commission to draft the regulation.⁷⁵ Amongst others, it was decided that data should remain in the system for on-line consultation for a period of at least five years. This period will start to run when the data of the decision on the visa application are entered in the system. After that period has elapsed, the data shall be deleted from the CS-VIS.⁷⁶

Data protection Directive 95/46/EC applies to the VIS. The European Parliament and data protection authorities have been involved in setting up a proper, separate legal framework. The European Parliament adopted on 22 April 2004 a non-binding resolution rejecting the current European Commission's proposal – presented on 12 February⁷⁷ – for the establishment of the VIS, and calling on the Commission to submit a more detailed document.⁷⁸ Also, in an opinion adopted in August 2004, the Article 29 Data Protection Working Party voiced a number of concerns regarding the proposed Visa Information System (VIS) and the inclusion of biometric elements in residence permits and visas for non-EU nationals.⁷⁹ Central concern of the Working Party *and* the

⁷³ Originally three options, were envisaged as biometric identifiers: iris scanning, facial recognition and fingerprints.

⁷⁴ Commission Communication to the European Parliament and the Council. 'Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)', *l.c.*, 25-26.

⁷⁵ European Justice and Home Affairs Council, *Conclusions*, 2561st Council meeting, Brussels, 19 February 2004, 5831/04 (Presse 37), 28p. via http://ue.eu.int/ueDocs/cms_Data/docs/pressdata/en/jha/79117.pdf

⁷⁶ European Justice and Home Affairs Council, *Conclusions*, 2561st Council meeting, *l.c.*, 19. Articles 92, 101 and 96.

⁷⁷ Commission of the European Communities, 'Proposal for a Council Decision establishing the Visa Information System (VIS), Brussels, 12 February 2004, Com(2004) 99 final, 22p.

⁷⁸ 'EU Data Protection Working Party expresses concerns about future Visa Information System' *eGovernment News*, 16 September 2004, 2p., via <http://europa.eu.int/ida/en/document/3284/330>

⁷⁹ Article 29 Data Protection Working Party, 'Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on

Parliament is the issue of centralizing the biometrical data. Neither the Commission document's, nor the Conclusions of the Council of Europe are clear about the issue of centralizing the biometrical data. On the contrary, the suggestion is made to establish such a database,⁸⁰ and made explicit in the Commission proposal for security features and biometrics in EU citizen's passports' of 18 February 2004 (*infra*).

In its opinion, the Working Party voiced important reservations – especially with regard to proportionality issues – about a solution that would lead to the storage of biometric data in databases. Indeed, this “would substantially increase the risk of the data being used in a manner that was disproportionate to or incompatible with the original purpose” for which the biometrics were collected. Such reservations are particularly motivated “when this data relates to traces that everyone leaves in their everyday life”, such as fingerprints, and when the databases are used for carrying out subsequent checks on individuals. In addition, the Working Party also stressed the “problems of reliability that could arise from the creation and interrogation of such a large database, and the potentially harmful consequences for the persons concerned”.

Summing up, like Eurodac, the current European Visa Information System (VIS) is a centralised database. The Council has proposed a Community Regulation (“visa code”) intended to consolidate and to a certain extent reform the existing Community provisions governing the granting of Schengen visas. The data subjects concerned are third country nationals from over a hundred different countries in the world that require a visa to enter the EU. Data on individuals can be kept for a five year period after the last expiry date of the visa or from the date that the application file was created if the visa is not issued. The database itself is operated by the European Commission (CS-VIS) and is connected via a communication network to the appropriate organizations in the Member States (NI-VIS). The responsibility for data control is split between the Commission and the Member States. Common Consular Instructions (CCI) has been amended to streamline the introduction of biometrics.⁸¹ The CCI biometrics introduces an obligation to collect biometrics from visa applicants and creates a legal framework for cooperation between Member States in processing visa applications. It does not provide the data subjects with their own data readable on a document for identification or verification. A biometric body check is thus the only possible way to use the system, thus again the human body is itself the tool for identification. This semi-mandatory ‘handing over’ of biometric information to a government agency sets similar ethical and technical questions as Eurodac. The database now holds biometric data in the form of

visas (VIS)' doc. 11224/04/EN WP 96, adopted on 11 August 2004, 12p. via http://europa.eu.int/comm/internal_market/privacy

⁸⁰ See in particular: European Justice and Home Affairs Council, *Conclusions*, 2561st Council meeting, *l.c.*, 19.

⁸¹ The Biodev I experiment conducted by Belgium and France in 2004/2005 has resulted in 180,000 biometric visa applications on the database.

digitalised photographs and fingerprints. Once adopted, the CCI biometrics proposal will be incorporated in the Visa Code. The choice of the Commission to deal with some issues relating to the use of biometrics in the CCI (such as the fingerprinting of children) rather than in the VIS has been challenged by the European Data Protection Supervisor (EDPS) and others.⁸² Objections have been made to the Commission's ability to determine exemptions of individuals or groups from the obligation to provide fingerprints. It is suggested that such exemptions should form an integral part of the VIS Regulation and not be decided by the Commission. This objection is based on two separate issues: guaranteeing democratic and transparent procedures and achieving legal clarity. The EDPS Opinion states:⁸³

“The EDPS objects... firstly, these provisions have a significant impact on the privacy of a great number of individuals and should be dealt with in the context of basic legislation rather than in instructions with a largely technical character. Secondly, the clarity of the legal regime would make it preferable to deal with this in the same text as the one establishing the information system itself”

In December 2006, it was proposed that Europol and other law enforcement agencies should gain access to VIS data under certain conditions. As in Eurodac there are some data protection safeguards in the form of defined access rights, responsibilities, confidentiality and security, and data subject rights. Data subjects (in this case the visa applicants) have the right to be informed about, amongst others, the purpose of VIS, the recipients of the data, the mandatory character of collecting the data and the right to access and correct data where it can proven to be incorrect. Before the collection of biometrics, only 30% of visa applicants used to go to consulates. The new biometric requirements mean that everybody must attend in person. This requirement is likely to mean that many applicants to make long journeys at considerable personal expense. Those unwilling to provide biometric data have only one option: a withdrawal from the visa application process and abandonment of the plan to visit the EU altogether. As with Eurodac, concern has been expressed about the reliability of biometric identification in visa applications.

4.4 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 2004.⁸⁴ In the Explanatory

⁸² See EDPS Opinion published December 2006 (C 321/38).

⁸³ See EDPS Opinion published on 27 October 2006 p 3.

⁸⁴ 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, 2Op.

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".⁸⁵ Following the events of 11/9 the need was felt to enhance the security of travel documents by adding biometric elements.⁸⁶ 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.⁸⁷ 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".⁸⁸

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.⁸⁹ The Council added a second mandatory biometric identifier to the proposal. 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.⁹⁰ In December 2004, the Council of European Justice and Home Affairs ministers adopted the regulation. The choice for mandatory facial images as well as finger scans and the idea of a centralized database was not questioned.⁹¹

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

⁸⁵ Commission of the European Communities, 'Proposal for a Council Decision on standards', *I.c.*, 2.

⁸⁶ *Ibid.*

⁸⁷ Commission of the European Communities, 'Proposal for a Council Decision on standards', *I.c.*, 6.

⁸⁸ Commission of the European Communities, 'Proposal for a Council Decision on standards', *I.c.*, 8.

⁸⁹ 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).

⁹⁰ Parliament report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizen's passports, including voting list and all amendments (25.11.2004), via http://www.edri.org/files/BioPass_AllAmend_VoteList.pdf

⁹¹ 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.

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.⁹² 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.⁹³

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.⁹⁴

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.⁹⁵

It remains striking how little attention has been paid by the EU institutions to publicly account for meeting the requirements of proportionality and necessity, the requirements that need to be met in the context of the human rights law (see above). 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.⁹⁶ Of course, part of the analysis overlaps. 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".⁹⁷ 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

⁹² Council Regulation of 10 December 2004, Annex, sub 3C.

⁹³ Council Regulation of 10 December 2004, Article 4, 1°.

⁹⁴ Council Regulation of 10 December 2004, Article 4, 2°.

⁹⁵ Council Regulation of 10 December 2004, Article 4, 3°.

⁹⁶ Commission of the European Communities, 'Proposal for a Council Decision on standards', *I.c.*, 6.

⁹⁷ *Ibid.*

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.

5. National Developments

5.1 Germany⁹⁸

5.1.1 Introduction

One of the first steps towards the use of biometrics by public authorities in Germany goes back to January 2002 when the German government adopted an act against terrorism (*'Gesetz zur Bekämpfung des internationalen Terrorismus'*) (*'TBG'*).⁹⁹ The TBG was passed to enable the use of biometric characteristics in passports and identity cards for German citizens as well as in identity cards for foreign citizens.¹⁰⁰

When the European Union agreed on the inclusion of biometrics in the electronic passport by Council Regulation No 2252/2004, Germany was among the first countries in Europe to issue a travel document containing a digital facial image as a biometric characteristic of its holder (*Elektronische Reisepass, ePass*) in November 2005. In June 2007, the German government decided on the immediate introduction of finger scans. As a result, the second generation electronic passports, including the fingerprint identifiers as well, have been issued since November 2007.¹⁰¹ Even though the above

⁹⁸ With thanks to Thomas Probst (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) for co-editing this section. These three country reports build on earlier work by the authors in the context of the FIDIS consortium, especially FIDIS Deliverable 13.4.

⁹⁹ *Terrorismusbekämpfungsgesetz* [Act against terrorism] of 9 January 2002 (BGBl. I S. 361, 3142), modified by Article 2 of the Act of 5 January 2007 (BGBl. I S. 2), available at <http://www.buzer.de/gesetz/4197/>

¹⁰⁰ T. Petermann, S., Scherz, and A. Sauter, 'Biometrie und Ausweisdokumente' [Biometrics and Identification Documents], *TAB Arbeitsbericht*, issue 93, 2003, p. 11. See for example article 7 (1) (b) and article 8 (1) in the aforementioned act, available at <<http://217.160.60.235/BGBl/bgbl1f/bgbl102003s0361.pdf>>, last consulted 18 March 2009. See also TAB working report 76, *Biometric Identification Systems*, available at <http://www.tab.fzk.de/en/projekt/zusammenfassung/ab76.htm>

¹⁰¹ There is an abundance of literature on the introduction of biometrics into the German passport. For some authoritative sources see: A. Albrecht, *Biometrische Verfahren im Spannungsfeld von Authentizität im elektronische Rechtsverkehr und Persönlichkeitsschutz*, Nomos, Baden-Baden, 2003; G. Hornung, 'Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues', *European Public Law*, vol. 11, issue 4, 2005; H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock, *White Paper zum Datenschutz in der Biometrie*, 2008, available at <http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf>. See also the implementation by the German home office, available at http://www.interoptest-berlin.de/pdf/Elbel_-_Experiences_in_introducing_the_new_German_ePassport.pdf

Council Regulation does not apply to identity cards, Germany has included biometric data on its electronic Identity Card (*Elektronischer Personalausweis*)¹⁰² as well: a digital facial image according to ICOA-standards (same as for ePass) is mandatory. Additionally, fingerprints can be stored on a voluntary basis.

5.1.2. Current Biometric Government Applications

As in the rest of the European Union, the traditional passports¹⁰³ in Germany are gradually being exchanged for the new digital passport, also called the ePass, in accordance with Council Regulation No 2252/2004. The Federal Parliament approved the introduction of electronic passports on 8 July 2005. Four months later, the first ePass was issued with the RFID chip containing only the facial image of the holder as the biometric feature. In June 2007, the Passport Act, which will be dealt with in more detail below, was again revised and approved by the parliament in order to lay down the legal foundation for the second generation electronic passports including additional finger scans (usually two index fingers) as biometric identifiers. These second generation electronic passports were issued in Germany from 1 November 2007 on.¹⁰⁴ Holders of these new passports thus carry a document with a chip containing their biometric data. These finger scans *are not stored centrally* but only stored on the RFID chip. This means that in case there is a suspicion that biometrics on RFID chips have been tampered with, the data cannot be compared to the originals as submitted at the moment of enrolment. The relevance of this will be discussed below. Another interesting observation in the past was that according to German officials, the data were hardly ever read out by German authorities, as the equipment to do so is currently not present or not used.¹⁰⁵ This has now changed. The automated border control was successfully tested and is going to be established permanently. With the "Easypass" technology, face data read from the electronic passports are automatically compared to pictures taken by a camera.¹⁰⁶ The scheme is due to be extended to the new National ID, containing biometric face scans and operative, as discussed below, since November 2010.

The German government has considered the advantages and disadvantages of the introduction of an electronic identity card (eID Card or Electronic Identity Card -

¹⁰² *Personalausweisgesetz* [Identity Cards Act] of 18 June 2009 (BGBl. I No. 33, 2009, p. 1346), available at <http://bundesrecht.juris.de/pauswg/>

¹⁰³ With traditional passports we refer to passports that in principle would not be read electronically (although such passport could be read electronically with scanning and optical character recognition (OCR)) and the passports that included already the Machine Readable Zone (MRZ).

¹⁰⁴ See also J-H. Hoepman *et al.* 'Crossing borders: security and privacy issues of the European E passport', *Advances in Information and Computer Security*. LNCS 4266, 2006, Berlin, Springer, pp. 152–167.

¹⁰⁵ Bundes Kriminal Amt Interview in November 2008. This statement has not been checked statistically as no such data are available.

¹⁰⁶ BioSig 2010 (<http://www.cast-forum.de/workshops/programm/131> and also <http://www.heise.de/security/meldung/Erfolgsgeschichte-EasyPass-soll-fortgeschrieben-werden-1076438.html>)

Elektronischer Personalausweis) for some time, launching a first feasibility study in 2003.¹⁰⁷ A second study was carried out by the Office of Technology Assessment (*‘Büro für Technikfolgenabschätzung’*), which had already submitted a first general report on biometric systems.¹⁰⁸ The Federal government adopted an electronic card strategy in a cabinet decision of 9 March 2005 aiming at the coordination of various projects (mainly ePass, electronic health card and the eID Card) carried out by different federal ministries.¹⁰⁹

The legal basis for the current paper-based identity cards (*‘Personalausweis’*) can be found in the Identity Card Act (*‘Personalausweis Gesetz’, ‘PAuswG’*). This act was revised, in order to provide for the introduction of the proposed eID Card. On 23 July 2008, the German cabinet decided on the wording of the law proposal for the new eID Card. It was agreed that, in addition to the traditional functions (photo ID, identification document, travel document), the new card would have *the functionality* to store biometric data (facial image/ finger scans) on the microchip. By including biometrics, the *use of the new eID Card as a travel document/passport* replacement could be guaranteed whilst the new features would also improve the card’s resistance against fraud. The proposed law passed the Parliament on 18th June 2009¹¹⁰. It is effective since 1st November 2011, when issuing of the new eID Card started. The validity of the ID cards (both the paper-based ID Cards prior to November 2011 as well as the new eID Cards) is ten years; limited to 6 years if the holder is younger than 24 years. As paper-based ID Cards remain valid, the last paper-based ID Cards will be replaced in 2021.

The inclusion of the facial image is mandatory while the inclusion of the *finger scans will be at the discretion* of the card holder. The card can store two finger scans. The inclusion of finger biometrics is therefore *optional*.¹¹¹ The law also contains a provision that biometric data *will not be stored centrally*.¹¹² When the index fingers are lacking or because of physical problems the quality of the scans is not sufficient, then a thumb, middle finger or ring finger is scanned. When as a result of a permanent medical condition no good quality scan can be obtained, the scan will not be stored on the chip¹¹³.

¹⁰⁷ G. Hornung, *l.c.*, p. 503.

¹⁰⁸ Büro für Technikfolgenabschätzung, ‘Biometrische Identifikationssysteme’ [Biometric Identification Systems], *Sachstandsbericht Bundestags*.

¹⁰⁹ IDABC, *eID Interoperability for PEGS: National Profile Germany*, available at: <http://ec.europa.eu/idabc/servlets/Doc?id=31524>, p. 17.

¹¹⁰ *Personalausweisgesetz PAuswG* [Identity Cards Act] of 18 June 2009 (BGBl. I No. 33, 2009, p. 1346), available at <http://bundesrecht.juris.de/pauswg>.

¹¹¹ *Personalausweisgesetz*: Section 5 (9) reads that the left and right index finger will be scanned and that the scans will be stored on the chip, when requested.

¹¹² *Personalausweisgesetz*. Section 26 (4).

¹¹³ *Personalausweisgesetz*. Section 5 (9). Sentence 3 and 4.

Biometric data from the eID Card cannot be read remotely without physical access to the document. Their use is only permitted to verify the identity of the holder (verification of biometric data between holder and those data stored in the chip of the eID Card) by specific public authorities (police, customs, registration authorities).¹¹⁴

While the image will also be stored also electronically at the registration offices (local authorities, about 5300 in Germany), this is not the case for the fingerprint images. They are stored in the chip of the eID Card only.

The eID Card will be the universal token for authentication and identification on the Internet for eGovernment and eBusiness services. The introduction of the eID Card can be considered as an important prerequisite for the eGovernment 2.0 programme, Germany's eGovernment strategy.

For the purposes above, features for electronic authentication and for digital signatures are implemented. The chip of the eID Card contains certificates to prove these data. Data from the chip can only be read if the holder agrees by entering a PIN beforehand (multi factor authentication). As the card shall be used for authentication in the private sector as well, and because in different contexts different parts of the total data are necessary, there will be a function to allow *the holder to control which data can be read* in a specific situation. For example, when a postal address is required, the date of birth and place of birth can not be read. When an age check is required, only the Boolean "passed"/"failed" is transmitted, not the date of birth. Additionally, also the entity which aims to read personal identification data from the eID Card is authenticated against the eID Card.

Specific certificates containing the desired data profile are used. Issuing and use of such certificates is limited by the following conditions: (1) the purpose for using the desired data is not illegal, (2) the data are not used for commercial data collections for the purpose of transfer (e.g., credit agencies) (3) the service provider has justified the necessity of using the data for the purpose of the transaction, (4) data protection law is adhered to, (5) and there are no indications that data abuse might take place.¹¹⁵

Additionally, the eID Card can hold a certificate for qualified electronic signatures¹¹⁶, as it is build as "secure-signature-creation device"¹¹⁷. Such certificates can be brought at non-governmental Certification Authorities.

¹¹⁴ Personalausweisgesetz, Section 17

¹¹⁵ Personalausweisgesetz. Section 21 (2) 1-5

¹¹⁶ That are *qualified certificates for advanced electronic signature* in the wording of Directive 1999/93/EC, Community framework for electronic signatures, Article 2 No. 2 and 10

¹¹⁷ Directive 1999/93/EC, Article 2 No. 6

The new identity card thus offers possibilities of an electronic identity proof for eGovernment and eBusiness applications. The new eID Card also contains a *pseudonym function*. The central idea is that the individual card number is used to generate a pseudonym that cannot be reconverted mathematically into the original card number. This pseudonym could then be used to register at web services that require authentication, but not personal identification.

In the semi-public domain, biometric applications are used in various places. In Spring 2010, a test of bodyscanners in Airport security started¹¹⁸ The currently tested devices are not used for recognition purposes, do not store any data, and show only a pictogram to the officers (instead of the semi-nude pictures of the first generation devices). There is however, a public discussion about the ethical implications of future applications in this field.

Already more contested, Deutsche Bahn (German Railway) has tested a facial recognition system at Mainz train station. Special cameras scanned the train station in search of 200 people who have volunteered to have their pictures stored in a database whose features can be detected by special biometric facial recognition software.¹¹⁹ All these initiatives have been reported to the German data protection authority, but very little is known about the extent to which they comply with the Directive 95/46/EC and German legislation in practice. There is some case law regarding the use of biometrics at work, but we have not come across other case law specifically dealing with the use of biometrics.

In 2005, BITKOM¹²⁰ conducted a study to develop a strategy for the German biometrics industry, and set up a national working group concerned with biometric issues, called *German Biometric Strategy Platform*. The study included the assessment of requirements, objectives, tasks and member structure of the German Biometric Strategy Platform.¹²¹ The report states that the two most important international factors influencing the German biometric industry are international *standardization* and

¹¹⁸ Of course at present a body scanner is not a biometric device at all, but some parallels are drawn with biometric devices as to the intrusion of bodily privacy. See: http://www.bundespolizei.de/cln_152/nn_249932/DE/Home/01__Aktuelles/2010/09/100927__koerperscanner.html, in German only).

¹¹⁹ http://www.cio.com/article/26000/German_ : "Railway_ Tests_Biometric_Technology".

¹²⁰ BITKOM represents more than 1,300 companies with combined sales of more than 120 billion Euro, with 900 direct members and around 700.000 employees, including practically all German global players as well as 600 key midsize companies in the information technology, telecommunications, and new media industry. The association's services comprise political consulting, public relations, knowledge management and other customized services.

¹²¹ BITKOM, *The German Biometric Strategy Platform: Biometric State of the Art, Industry Strategy Development and Platform Conception*, Berlin, 2005, available at http://www.europeanbiometrics.info/images/resources/95_363_file.pdf ('BITKOM, *The German Biometric Strategy Platform*')

security policy efforts.¹²² According to the report, the German federal government is the most important driver for biometric technologies in Germany. It takes a position as promoter and customer – on the one hand it seeks to support the industry with a national, seller-independent economic policy, and on the other hand it is expected to be the first major German customer for biometric applications. Moreover, federal and Länder authorities are involved in the biometric standardization process.¹²³ Compared to other countries, the public perception of biometrics in Germany is strongly influenced by ethical questions.¹²⁴ This translates itself also into a more principled stance on the use of biometrics. The clearest example of this is a general agreement on the fact that a central database containing biometric data would be unconstitutional and be a violation of basic rights.¹²⁵ The possibility of a *nationwide database has already been ruled out by the German legislation* relating to the ID card in 2002.¹²⁶ The compatibility of the idea of a central data base with the German Constitution will be discussed further below.

5.1.3 Legislation

Three so-called ‘first pillar’ instruments govern the EU data protection framework: the general Directive 95/46/EC which has been implemented in Germany through the Federal Data Protection Law (*‘Bundesdatenschutzgesetz’, ‘BDSG’*)¹²⁷, the specific Privacy and Electronic communications Directive 2002/58/EC¹²⁸ transposed in the Telecommunications Act (*‘Telekommunikationsgesetz’, ‘TKG’*¹²⁹) and Telemedia Act (*‘Telemediengesetz’, TMG’*¹³⁰) and the Regulation No 45/2001 of the European Parliament and of the Council of 18 December 2001 on the protection of individuals

¹²² BITKOM, *The German Biometric Strategy Platform*, p. 24.

¹²³ *Ibid.*, p. 35.

¹²⁴ BITKOM, *The German Biometric Strategy Platform*, p. 24.

¹²⁵ See also Z. Geradts, ‘Forensic implications of identity systems’, *Datenschutz und Datensicherheit*, 2006, 30, pp. 556–558.

¹²⁶ See Footnote **Fout! Bladwijzer niet gedefinieerd.** on the Terrorismusbekämpfungsgesetz in 2002. It contained changes for the Personalausweisgesetz (Identity Card Act), allowing the use of biometric data in ID Cards and passports, but prohibiting a nationwide data base. This possibility was not used; instead, in 2008/2009 the ID Card was designed as an eID Card, see above.

¹²⁷ This act came into force in 1977 and was revised in 2001 to integrate the Data Protection Directive 95/46/EC into the German framework. For a translation of the Act see: http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

¹²⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O. J. L* 201, 31 July 2002. Article 3 §1 states: ‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community’.

¹²⁹ http://bundesrecht.juris.de/tkg_2004/

¹³⁰ <http://bundesrecht.juris.de/tmg/>

with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.¹³¹

As stated above, the Directive 95/46/EC constitutes the main and general legal framework for the processing of personal data. For a general discussion of the provisions of the Directive in relation to biometrics see the general section above.

National regulators have a considerable margin of appreciation when evaluating biometrical issues. This can be explained by the fact that most national data protection laws implementing the Directive 95/46/EC contain no specific provisions or criteria on the processing of biometric data. This observation certainly applies to the German legal framework that contains no specific laws or regulations on the use of biometrics. The most important general requirement is the protection of human dignity according to Article 1 of the German Constitution ('*Grundgesetz*' '*GG*'). This article stipulates that 'Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority'.¹³² Furthermore, in Germany, as elsewhere in Europe, the application of biometrics is predominantly governed by general data protection laws.

In Germany, the Federal Data Protection Law, controls the storage, processing and use of personal data collected by public federal and state authorities and by private parties, the latter in case they process and use data for commercial or professional aims. The Federal Data Protection Law is the most important law for the processing of biometric data and contains rights and obligations with respect to data protection. The Federal Data Protection Law stipulates the following principles: proportionality, purpose specification, and data reduction and data economy. This means that it has to be guaranteed that only data are collected or used, which are necessary and which are permitted by the law.¹³³ Although there is no German case law dealing specifically with the handling of biometric data, there is some publicly available data protection advice on the application of the various laws to biometrics and the choices that can be made for privacy enhancing variations of the technology.¹³⁴

¹³¹ O. J. L 8, 12 January 2001.

¹³² <http://www.iuscomp.org/gla/statutes/GG.htm>

¹³³ For more details, see section **Fout! Verwijzingsbron niet gevonden.** of this deliverable or E. Kindt in: , *Datenschutz und Datensicherheit (DuD)*, 2007, 31, pp. 166-170.

¹³⁴ See the publications by Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, available at <https://www.datenschutzzentrum.de/projekte/biometrie/kap6krit.htm>; <https://www.datenschutzzentrum.de/projekte/biometrie/index.htm>; see also Datenschutz Berlin, available at <http://www.datenschutz-berlin.de/content/themen-a-z/biometrie/biometrische-authentisierung>; and the website of: <http://www.datenschutz.de/>. In addition, and apart from FIDIS publications, see other academic literature, for example, L. Donnerhacke, 'Anonyme Biometrie', *Datenschutz und Datensicherheit* 1999, Vol. 23 , Nr. 3, S. 151-154; M. Köhntopp, 'Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren', Horster (ed.), *Sicherheitsinfrastrukturen*, Vieweg, Braunschweig 1999, sections 177-188; A. Pfitzmann et al., 'Trustworthy User Devices', Müller and Rannenber (eds), *Multilateral Security in Communications*, Addison-Wesley, München 1999, sections 137-156.

Finally, the German Constitution (*‘Grundgesetz’*) includes the right to informational self-determination (*‘Recht auf informationelle Selbstbestimmung’*). At first it was argued by most commentators, that a central database (or its de-central equivalents) would be incompatible with this right.

However, the strict legal interpretation of this principle seems to come under some pressure.¹³⁵

One significant and recent case on the issue of central storage of personal data of the European Court of Justice relates to a preliminary question of a German court. The background, the Court’s reasoning and the implications of the case have been discussed above in section **Fout! Verwijzingsbron niet gevonden..** The German Act relating to a Central Register of Foreigners Act (*‘Gesetz über das Ausländerzentralregister’*)¹³⁶ has established a centralised register which contains certain personal data relating to foreign nationals who are resident in Germany for a period of more than three months. From 2005, The Federal Office for Migration and Refugees (*‘Bundesamt für Migration und Flüchtlinge’*) is responsible for maintaining that register.¹³⁷ There are around 7 million permanent inhabitants in Germany that do not have the German nationality. The register is used for statistical purposes by security and police services and judicial authorities in exercising their powers in relation to the prosecution and investigation of criminal activities which threaten public security. In its ruling, the Court of Justice stated in an answer to the preliminary questions that the centralisation of the data does not satisfy the requirement of necessity laid down in the Directive 95/46/EC.

The design and the use of the identity card and passport are regulated in respectively the Identity Card Act (*‘Personalausweis Gesetz’, ‘PAuswG’*) and the Passport Act (*‘Passgesetz’*), which has already been discussed to some extent above.

With regard to biometrics, Article 7 of the Act against terrorism (*‘TBG’*) (see *above*) added a new paragraph 23a to the Passport Act that allows the use biometrics in the German passport.¹³⁸ Meanwhile, the Passport Act was revised.

The authorities responsible for the identity cards (the citizen’s registration offices at the *municipality level*) keep records on identity cards.¹³⁹ Among others, these local registries issue the identity cards and verify their authenticity. Every identity card has a unique

¹³⁵ G. Hornung, ‘The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards’, *SCRIPTed* vol. 4, issue 3, 2007.

¹³⁶ *Gesetz über das Ausländerzentralregister* (*‘AZR-Gesetz’*) of 2 September 1994 (BGBl. I S. 2265), recently modified by Article 2 of the Act of 26 February 2008 (BGBl. I S. 215). See <http://www.gesetze-im-internet.de/bundesrecht/azrg/gesamt.pdf>

¹³⁷ See

http://www.bamf.de/cln_092/nn_441806/sid_4914EA581C5A6781FB012BA5814E3264/SharedDocs/Pressemitteilungen/DE/DasBAMF/2005/050629-pressemitteilung-07-05-bamf.html?__nnn=true

¹³⁸ See also Article 11 TBG which changes the foreigner law (*Ausländergesetz, AuslG*) and provides for the integration of biometrics in visas and residence permits of foreigners.

¹³⁹ *Personalausweisgesetz*, Section 23.

serial number. It is explicitly forbidden to use this number for accessing personal data in files or for linking data in different files.¹⁴⁰

The passport register, regulated by the Passport Act, is controlled by the passport authorities (again, the *citizen's registration offices at the municipality level*). They issue passports and verify their authenticity, as well as the identity of the person who owns the passport or for whom it has been issued. Besides authorizations for respective police, customs and registration authorities, the Passport Act explicitly stipulates that the use of biometric data is strictly *limited to verification and authentication* of the passport and the identity of the holder (purpose specification).¹⁴¹ Careful reading indicates that the fingerprint data are not stored on a database, but only on the passport itself.¹⁴² In the future, only other Nations granted permission by the Federal Republic of Germany (in the form of a special cryptographic certificate to be used in electronic Passport reading devices) will be able to access the microchip's data of the ePass.

As already mentioned above, *a nation-wide database*, hence not only a biometric database, is *explicitly forbidden by the legislator in the German Passport Act (Section 4 (3))*. Biometric facial data can be preserved in a local database.¹⁴³ As regard to fingerprints, the 2007 revision of the Passport Act stipulates that finger scans are to be stored exclusively on the passport's microchip, and that they should in no case be stored locally or in a central database. Subsequent the scanning and use of the finger scan data the authorities are obliged to delete the data.

5.1.4 Data Protection Authorities and Biometrics

The federal oversight is executed by the Federal Data Protection and Freedom of Information Commissioner who controls that all federal agencies comply with the data protection legislation.¹⁴⁴ Chapter 3 of the FDPL provides the legal basis for the Commissioner and outlines his functions. The key role is to ensure that the Data Protection Act is implemented correctly. Section 24 states that the Commissioner has to monitor compliance with the Act and grants him powers of access to information as well as the opportunity to inspect all documents and the right of access to all official premises at any time. Section 25 stipulates that the Commissioner can lodge complaints with higher authorities (e.g. the competent supreme federal authority) in the case of

¹⁴⁰ Personalausweisgesetz, Section 20 (2), 20 (3)

¹⁴¹ Passgesetz (Passport Act) from 1986, last change 30 July 2009, (BGBl. I 2009 S. 2437), Section 16.

¹⁴² See Passgesetz Section 16 (2): Deletion of finger prints after issuing of the document. The digital face picture, however, will be stored by the passport register in the same way as a second paper based photo was stored in the past.

¹⁴³ Most of these local databases, the citizens registers, however, would be centrally accessible via an XML-interface. So technically there is no big difference to a central database in case of an authorised access e.g. by police forces e.g. in cases of ongoing investigations is needed

¹⁴⁴ http://www.deutschland.de/link.php?lang=2&link_id=24

breaches. In Section 26 it is laid down, inter alia, that the Commissioner can be requested by federal government to give opinions and make recommendations on matters pertaining to the law. The FDPL also sets out the penalties for breaches in Sections 43 and 44.1. They are fines and imprisonment.

However, as the Federal Republic of Germany is a federation of 16 States (*Bundesländer*)¹⁴⁵ the competences of the State are divided between the federal and the State governments. The federal system of government, with its clear division of powers between the governments of the States and the federal government also affects the supervision of data protection. Therefore, there is number of different authorities that are responsible for making sure that data protection laws and regulations are complied with. Thus German Federal States have their own DPAs, which are responsible for controlling the observance of data protection legislation by public bodies located in their jurisdictions.¹⁴⁶ There is no uniform system for the supervision over the private sector in the individual states. In some States, the supervisory functions are performed by the Ministry of Home Affairs or by the authorities that report to the Ministry. In other States, e.g. North Rhine-Westphalia, supervision is exercised by the DPA.¹⁴⁷ A private company is supervised by the authority that has jurisdiction over the district where it has its headquarters.

This country study has provided a short overview of all relevant aspects and issues surrounding the use of biometrics in Germany. Clearly, a pivotal event in this regard was the introduction of the ePass in Germany. The introduction of the passport, so soon after the EU Regulation 2252/2004, was the result of independent German government deliberations about the introduction of biometrics since 2002. Initially, the ePass contained only a facial image as a biometric identifier, but as of June 2007 the German government approved the inclusion of finger scans. As a result, the second generation electronic passports, with EAC and including the fingerprint identifiers have been issued since November 2007. The fingerprint identifiers, however, are by law stored exclusively on the passport's microchip, and not stored locally in the citizens' registers or in a central database.

The eID Card as introduced contains a mandatory electronic facial image, whilst the inclusion of fingerprints will be at the discretion of the citizens. The aim is to implement the eID Card as a universal token for authentication and identification on the Internet for eGovernment and eBusiness services.

¹⁴⁵ These States ('Bundesländer') are not just provinces but states with their own original sovereign rights and legislative responsibilities.

¹⁴⁶ For a list see: https://www.lidi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Datenschutzbeauftragte/Datenschutzbeauftragte.php

¹⁴⁷ For a list see https://www.lidi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Aufsichtsbehoerden/Aufsichtsbehoerden.php

As for the regulatory framework, there are no specific regulations or laws concerning biometrics in German law. The Federal Data Protection Law, which covers the storage, processing and use of personal data collected by public federal and state authorities and by private parties, serves as a framework for the handling of biometric data. A nationwide database, with data relating to the passports, hence not only a biometric database, is explicitly forbidden by law (Section 4 (3) Passport Act). Biometric facial data can be preserved in a local database, while finger scans are stored exclusively on the passport's microchip thus excluding any local or central storage.

5.2 United Kingdom

5.2.1 Introduction

Unlike most of the other EU Member States, the UK did not participate in the decision making around the Council Regulation 2252/2004 which introduced the European electronic passport with biometric identifiers. This Regulation was adopted in the context of Schengen, in accordance with Council Decision 2000/365/EC. As such, because the UK does not take part in Schengen, there was no obligation on the UK to introduce biometrics, in particular biometric fingerprint.¹⁴⁸ Nevertheless, in line with international developments, the British government prepared for the introduction of biometrics into UK passports. More importantly, the previous UK government made it clear with the proposed National Identity Register (NIR) that it intended to take the use of biometrics in identity management to an unprecedented large-scale. The new coalition government, formed after the elections in May 2010, has put most of these plans on ice, and is conducting a review.¹⁴⁹

5.2.2. Current Biometric Government Applications

In December 2003, the Parliamentary Under-Secretary for the Home Office listed the *government projects* that do or will make use of biometrics. The list was presented in an answer to a parliamentary question. The projects were listed in what seems to be an order of importance: the inclusion of the first and second biometric identifier in the British passport; biometric identifiers in the identity cards programme; the UK visas biometric programme; biometric travel documents; biometric residence permit; IAFS (Immigration and Asylum Fingerprints System); the e-Borders programme; the PITO project to use face recognition to support FIND; LANTERN (a mobile fingerprint system) and the national DNA database. In addition, the Under-Secretary of State listed some

¹⁴⁸ The UK is, however, an ICAO member and the ICAO document 9303 for Machine Readable Travel Documents binding. This document provides for the inclusion of a digital photograph on a contactless chip, while an addition biometric identifier, such as fingerprint, remained optional.

¹⁴⁹ BEST Deliverable 7.1. Biometrics in Europe: Inventory on politico-legal priorities in EU27, prepared by Juliet Lodge, pp 32ff.

smaller projects involving the Home Office: IDENT1, Application Registration Cards (ARC), ISRP, VIAFS, IRIS, C-Nomis, pilot of methadone dispensing system using iris recognition at HMP Eastwood Park, and a trial of fingerprint based access control to IT systems in prisons.¹⁵⁰ Participation in most of these government projects is *mandatory*. Of course, the decision to request a passport or identity card can be framed as voluntary. However, given the fact that many government services cannot be obtained without passport or identity card, this is a theoretical argument.

The UK national identity system, also called the National Identity Scheme (NIS), was the main government initiative with regard to the use of biometrics in the UK. The scheme, based on the Identity Cards Act passed in March 2006, would provide a comprehensive way of recording personal identity information, storing it and making it possible to use it if one wants to prove his or her identity. The NIS would apply to all those over 16 years old, including foreign nationals, who legally reside or work in the UK.¹⁵¹ Notwithstanding the title of the Identity Cards Act, the basis of the Act would not be the ID card but a *database*, (The National Identity Register ('NIR') containing information relating to individuals. The ID card would only be issued after the required "registrable" facts have been entered into the NIR.¹⁵² A registrable fact in relation to an individual included personal information defined as 'his full name', his other names by which he is or has been previously known, date and place of birth, date and place of death and 'external characteristics of his that are capable of being used for identifying him'.¹⁵³ The term 'identifying information' was also used in the Identity Cards Act and applied to biometric data especially. The Act referred to a photograph of head and shoulders, fingerprints and 'other biometric information' as well as to a handwritten signature. Iris scans were not mentioned in the Act.

By using the term 'identifying information' as a label for biometric data, the UK legislator showed that it places its trust primarily on biometrics for the authentication of identity.¹⁵⁴

The identifying information (including biometric data) was recorded in Schedule 1 that contains eight other categories of information.¹⁵⁵ When a person enrolls, biometric

¹⁵⁰ See <http://gizmonaut.net/blog/2006/12/03>

¹⁵¹ Identity Cards Act 2006 ('Identity Cards Act') section 2 (2)(b). The Identity Cards Act can be consulted at < http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060015_en.pdf>.

¹⁵² Identity Card Act section 6 (6) and (8).

¹⁵³ Identity Card Act section 7 (1).

¹⁵⁴ The website for example explains: 'Your biometrics will be permanently paired with your biographical information to create completely unique and secure identity data'. See <http://www.ips.gov.uk/identity/scheme-what-produced.asp>

¹⁵⁵ This information is: the fore mentioned personal information, residential status, personal reference numbers, record history, registration and card history, validation information, security information and records of provision of information. It is important to note that the categories of information in the register can be changed at a later date: under the Act section 3(6) the Secretary 'may by order modify the information for the time being set out in schedule 1'. Under section 3 (7) of the Act, the draft order must be laid 'before Parliament and approved by a resolution to each House'.

information (e.g. facial image, fingerprints) will be recorded, and there are mobile and local centres that are equipped to register these kinds of data. The basic identity information would be recorded and maintained on the NIR. The NIR would thus contain only identity-related information.

The first cards were issued in 2008. NIS was a long-term programme which would take several years before it would become fully operational. The former UK government envisaged that the scheme would protect the public against identity theft and fraud. Other expected benefits included increased safety, through protection of the community against crime, illegal immigration and terrorism, and reassurance that workers in positions of trust, such as those working at airports, are who they say they are. The big problem for the UK has been slack data processing and management practices, with considerable loss of data through carelessness or theft. The public finds government claims to be disingenuous.¹⁵⁶

The scheme, as set out by the previous government, came immediately under fierce criticism by the new government in May 2010. Straight away, the deployment of obligatory government controlled biometric applications such as biometric visas, enhanced passports and identity cards, apart from those cards issued to foreign nationals in the form of biometric immigration documents, came to be scrapped. The new Government introduced the Identity Documents Bill to Parliament on 26 May 2010. The Bill made provision for the cancellation of the UK National Identity Card, the Identification Card for EEA nationals and the destruction of the National Identity Register. The identity card for foreign nationals (biometric residence permit) is not being scrapped for the time being.¹⁵⁷

In March 2006, the UK made a transition from digital to electronic passports (ePassports) in order to comply with the US Visa Waiver Programme and other international requirements.¹⁵⁸ The main aim was to strengthen border controls. The ePassport contains an electronic chip storing biographical data and a digital facial image of the passport holder. The chip can be read using an appropriate electronic reader located at border control.¹⁵⁹

¹⁵⁶ BEST Deliverable 7.1. Biometrics in Europe: Inventory on politico-legal priorities in EU27.

¹⁵⁷ See Home Office Identity and Passport service:

http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xml/53.htm

¹⁵⁸ House of Commons Committee of Public Accounts, Identity and Passport Service: Introduction of ePassports, available at <http://www.ips.gov.uk/passport/downloads/Introduction_of_ePassports.pdf>, last consulted 23 February 2009, p. 7.

¹⁵⁹ The ePassport was the first official UK document to incorporate an electronic chip in a paper document and it incorporates technically advanced security features to make it harder to forge and prevent unauthorised reading of the chip.

To conform to other EU requirements specifying that electronic passports within the EU should include a second biometric identifier in addition to the face scan (digital photograph) by 2009, the UK plans to issue second generation ePassports soon.¹⁶⁰ These passports will store the holder's finger scans on the chip.¹⁶¹ Although the chip units (chip, its operating system, the antenna and the plastic covering in which it is housed) have been tested in laboratory conditions, their ability to withstand real-life passport usage is unknown.¹⁶²

Next to the identity card and the ePassport, the UK is also using biometrics in other government controlled applications. When viewed in the light of the list of the Parliamentary Under-Secretary for the Home Office in 2003,¹⁶³ apart from the introduction of the NIR, the most important biometric applications used by the British Government have not changed since then. The three major ones are hereunder briefly described:¹⁶⁴

- Through the UK visas Biometrics Programme, biometric visas (fingerprints) are being issued to *foreign nationals* who wish to enter the UK and *require an entry visa*. The programme covers three quarters of the world's population and operates in 135 countries. More than one million fingerprint scans have been completed.
- The UK Border Agency operates the Iris Recognition Immigration System (IRIS) at some UK airports which provides a fast, secure and convenient way for *foreign and returning UK travellers* to enter the UK.
- The fingerprints of *asylum* seekers are recorded when they register for an Application Registration Card (ARC).

In general, DNA (deoxyribonucleic acid) is not considered a biometric (see above section 3.5). At the same time, DNA also contains information that will uniquely identify a certain person. Because of that reason, and because of major (worldwide) attention for this database, we nevertheless discuss hereunder the in the UK existing DNA database.¹⁶⁵

¹⁶⁰ As stated above, the UK is not obliged to comply with the EU regulations as it is not a signatory of the Schengen Agreement. Nevertheless it has decided to participate on a voluntarily basis. This secures participation in the development of the EU regulations in this area and helps maintain the security of the British passport on a par with other major EU nations.

¹⁶¹ Although planned for 2009, there may be a slight delay in including finger scans in British passport chips. The reasons for this delay have not been made public.

¹⁶² In the UK, there have been reports of doubts on the durability and reliability of the chip units used. British ePassports are intended to last ten years but the RFID chip units used only have a two year warranty. Compare also with footnote **Fout! Bladwijzer niet gedefinieerd.**, p 2.

¹⁶³ See <http://gizmonaut.net/blog/2006/12/03>

¹⁶⁴ Biometrics Assurance Group, *Annual Report 2007*, available at <
http://www.ips.gov.uk/passport/downloads/FINAL-BAG-annual-report-2007-v1_0.pdf>, last consulted February 2009, p. 4.

¹⁶⁵ We will not discuss the interface between bio banks and the storage of biometric(s) (templates). This has been done elsewhere. See http://www.jus.uio.no/iri/om_iri/seminarer/Bodycontrol.html

The national DNA database (NDNAD) in the UK (comprising in this instance England & Wales and Northern Ireland; Scotland has a separate DNA database with different rules) is the largest in Europe, with liberal rules for taking and retaining DNA samples and profiles compared to other European countries. It is possible in the UK to retain bodily samples and DNA profiles upon arrest for any offence, regardless of whether a charge and conviction follows. With the DNA of 940,000 people on file the UK has the most “profiled” population in the world.¹⁶⁶ Recently, there have been a number of significant developments in the use of DNA profiling techniques in law enforcement. The government has announced an increase in funding to enable the UK DNA database to be more rapidly expanded – at the end of 2008 the number of profiles held was rising at the rate of 6,000 per week.

In view of the fact that EU Member States have already started exchanging DNA profiles, all profiles collected in the UK can potentially be used by authorities in other EU Member States. By its Decision of 23 June 2008,¹⁶⁷ the European Council agreed to integrate the main provisions of the Prüm Convention into the EU's legal framework, to enable wider exchanges (between all EU Member States) of biometric data (DNA and fingerprints). All EU Member States will therefore be required to set up DNA databases. The Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters – is the first general data protection instrument in the EU third pillar.¹⁶⁸ In this decision the option of a future European database is not excluded.

In the UK, police are only allowed to keep DNA profiles on the national database from people who are convicted of the offence for which the sample was taken. All other samples must be destroyed. However, a Home Office Inspectorate of Constabulary report, ‘*Under the Microscope*’, estimated that from 752,718 DNA profiles held at the time of their study, those of 50,000 individuals which should have been destroyed have been retained.¹⁶⁹ This figure was based on a non-conviction rate of 20%.¹⁷⁰

¹⁶⁶ In September 2008, the government announced an extra £109 million to expand the database (this comes after the extra £34 million announced in September 1999).

¹⁶⁷ 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 and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ L 210*, 6.8.2008.

¹⁶⁸ See above, section **Fout! Verwijzingsbron niet gevonden..**

¹⁶⁹ Home Office, *Under the Microscope*, available at <

<http://inspectors.homeoffice.gov.uk/hmic/inspections/thematic/utm/microsco.pdf?view=Binary>>

¹⁷⁰ According to Statewatch (<<http://www.statewatch.org/news/2008/dec/uk-dna-database-background-article.pdf>>), more realistic figures would be non-conviction rates of 33 and 45% - suggesting that 82,UK 500-112,500 DNA profiles should actually have been destroyed.

There have been individual court cases about illegally retained DNA samples. In 2008, Michael Weir's conviction for murder was quashed at the Court of Appeal. Weir had been convicted on the strength of DNA evidence based on blood found on a glove.¹⁷¹ The Court affirmed the rules of the Police and Criminal Evidence Act 1984 which state that *'information derived from the sample of any person entitled to its destruction [...] shall not be used - (a) in evidence against the person entitled; or (b) for the purposes of any investigation of an offence. If the sample was used for purposes of an investigation then all evidence resulting from that information must be excluded.'*¹⁷²

There is also a case pending involving three Police Federation backed police detectives who object to having been assigned desk-jobs as a result of failing to provide a voluntary sample.¹⁷³

The last case to be mentioned here is the European Court of Human Rights judgment of 4th December 2008, in the case of *S. & Marper v. the UK*.¹⁷⁴ The ECHR Grand Chamber (GC) found unanimously that the retention by the police of fingerprints and DNA samples from a man and a boy arrested, but not convicted, violated their right to privacy. The judgment provides a landmark decision setting limits to the growth of national DNA databases in general, and that of the UK in particular. The case had previously been rejected by the House of Lords, which had placed the importance of crime detection above issues of data privacy. The applicants had subsequently applied to Strasbourg under Article 8 (the right to privacy) and Article 14 (non-discrimination).

5.2.3 Legislation

The national legal privacy framework for biometrics is the Data Protection Act 1998, which came into force in March 2000 (hereinafter the 'DPA 1998') which is in principle applicable to the collection and processing of biometric data. However, the DPA 1998 does not contain specific provisions which mention biometric data as such.

¹⁷¹ The police matched the blood to a DNA sample taken from Weir a year previously when he was suspected of drugs offences. At the time, he had not been charged. Nevertheless, his profile was placed in the national register.

¹⁷² Section 64 (3B) of Police and Criminal Evidence Act 1984.

¹⁷³ According to Statewatch (<<http://www.statewatch.org/news/2008/dec/uk-dna-database-background-article.pdf>>) UK the Home Office has confirmed that at least 50,000 people's DNA profiles are held illegally, but are yet to state what is being done about it.

¹⁷⁴ For the implications and the arguments in the case, see *above* and at <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>. That there were fundamental issues at stake is reflected in the fact that the case was put before the 17 judges of the Grand Chamber. It shall be particularly noted here that the Court gave a very broad definition to the concept of privacy within the meaning of Article 8 – the right to privacy. The Court had no hesitation in viewing fingerprints and DNA samples as falling within the ambit of Article 8. For the original case see: *Regina v. Chief Constable of South Yorkshire Police ex parte LS/ ex parte Marper* [2004] UKHL 39, <http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040722/york-1.htm>

There are a number of separate instruments at the national and international level that would apply to certain aspects of the use of biometrics. As apart from DNA cases, there are no cases involving biometrics yet. Therefore, an analysis will have to be carried out on the basis of existing case law involving personal data.

As stated above, according to Art 3 (2) and recital 13, the Directive 95/46/EC does not apply to the processing of data in the course of an activity which falls outside the scope of European Community law, such as provided for by Titles V (provisions on common foreign and security policy) and VI (provisions on police and judicial cooperation in criminal matters) of the Treaty on European Union. Activities that are processing operations concerning public security, state security and the activities of the state in areas of criminal law therefore all fall outside the scope of the Directive.

Certainly, all matters relating to passports and national ID cards are not regulated by the Directive 95/46/EC and find their legal basis in UK legislation. For example, as already discussed above, the legal base for biometric data processing has been a major issue in the build-up to the adoption of the Identity Cards Act 2006.¹⁷⁵

It is clear that beyond the directly applicable national legal framework, the right to privacy and the use of biometrics is complex. This applies especially to the use of biometrics in the context of the fight against terrorism.

The ICO has proposed some legal measures to further protect private data, also with a view to possible security lapses that concern biometric data. In his evidence to the House of Commons Justice Committee inquiry into the protection of private data, the ICO made two specific proposals.¹⁷⁶ The first is to give the ICO the power to force data holders to commission *an independent audit* of their procedures. The second is a requirement for bodies to notify the ICO or a similar body, when a major and potentially *dangerous privacy breach* has occurred, as well as notifying the individuals who may be affected. The UK government plans to increase penalties for trading in personal data, from a fine as currently set to two years imprisonment under new penalties in the Criminal Justice and Immigration bill.

5.2.4 Data Protection Authority and Biometrics

At the top of the UK Information Commissioner's home page, the mission of the ICO is stated as follows: 'the UK's independent authority set up to promote access to official information and to protect personal information'.¹⁷⁷

The House of Commons Home Affairs Committee has issued a report on the Surveillance Society¹⁷⁸ which was discussed above. In his response to the report, the ICO supported

¹⁷⁵ See for example the abovementioned *The Identity Project*.

¹⁷⁶ House of Commons Justice Committee, *Justice – First Report*, available at <<http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf>>, last consulted 11 March 2009.

¹⁷⁷ See the site www.informationcommissioner.gov.uk.

the proposal that the Home Office should submit *contingency plans for the loss of biometric* information to ICO.¹⁷⁹ The Committee also recommended that the Home Office should address ICO concerns on administrative information collected as part of the National Identity Register (paragraph 248 of the Report). In its reply, the ICO stressed its continuing concern that the amount of information is *to be kept to the minimum* with administrative information deleted as soon as it has served its purpose. The ICO states it is particularly concerned about the 'audit trail' data and wants this minimised, access restricted and early deletion.¹⁸⁰ In its reply, the ICO also supported the Committee's recommendation that the Home Office submits detailed plans for *securing NIR databases and contingency plans* for the loss of biometric information to ICO for comment (paragraph 246 of the report). The ICO confirmed that it would welcome the opportunity to provide comments on the data protection implications of the Home Office and IPS plans.¹⁸¹

In January 2009, the ICO forced the Home Office to sign a *formal declaration* promising to hold personal data securely in the future.¹⁸² With immediate effect, all portable and mobile devices which are used to store and transmit personal information must be *encrypted*. The case in question occurred in August 2008 when a Home Office contractor, PA Consulting, lost an unencrypted memory stick holding sensitive personal details of thousands of people serving custodial sentences or who had previously been convicted of criminal offences.¹⁸³

¹⁷⁸ Constitution Committee, *Fifth Report session 2007-2008: A surveillance Society?*, available at <<http://www.publications.parliament.uk/pa/ld200708/ldselect/ldconst/44/44.pdf>>, last consulted 11 March 2009.

¹⁷⁹ House of Commons Home Affairs Committee, *A Surveillance Society? Information Commissioner's Response to the Committee's Fifth Report of Session 2007-08*, available at <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/1124/1124.pdf> , last consulted 11 March 2009, p. 6.

¹⁸⁰ *Ibid.*, para. 6.8.

¹⁸¹ *Ibid.*, para 6.7

¹⁸² The ICO has ordered a number of organisations to sign undertakings following breaches of the Data Protection Act. These include the Department of Health, Foreign and Commonwealth Office and Orange Personal Communications Services Ltd.

¹⁸³ Mick Gorrill, assistant Information Commissioner, issued the following statement: "This breach illustrates that even though a contractor lost the data, it is the data controller (the Home Office) which is responsible for the security of the information. It is vital that sensitive personal information is handled properly and held securely at all times. The Data Protection Act clearly states that organisations must take appropriate measures to ensure that personal information is kept secure. The Home Office recognises the seriousness of this data loss and has agreed to take immediate remedial action. It has also agreed to conduct future audits to ensure compliance with the Act. Failure to meet the terms of the Undertaking is likely to lead to further enforcement action by the ICO". See <http://www.karoo.co.uk/article.asp?id=18987429&cat=headlines>. See also Information Commissioner's Office, *ICO takes enforcement action against NHS Trusts for data losses*, available at <http://www.ico.gov.uk/upload/documents/pressreleases/2009/nhs_trusts_undertakings_final.pdf>, last consulted 11 March 2009.

5.3 The Netherlands

5.3.1. Introduction

The Dutch government started up a policy process aiming at the introduction of biometrics in identity documents before this was agreed at the European level. We have seen a gradual rolling out of biometric applications in the Dutch public sector. The main government policies in this regard are the introduction of face and finger scans into the Dutch passport, identity management using biometrics within the criminal justice system (Progis)¹⁸⁴, and the use of biometrics for the registration and identification of foreigners (in visa, residence permits and political asylum and immigration procedures). Of these examples, only the use of biometrics in the criminal justice system is not in direct parallel with developments in the EU. All the other government applications that are being introduced have been initiated, or at least re-enforced by decisions made at EU level about machine readable documents.¹⁸⁵ Therefore, although the introduction is gradual, in a few years time the majority of people living in the Netherlands will have become enrolled in a government biometric application. In one of our empirical studies¹⁸⁶, we found that it proved impossible to draw up a reliable inventory of all biometric applications in the Netherlands. The Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, 'CBP') keeps a register of all projects notified under the data protection legislation¹⁸⁷, but in the current set up, the biometric projects are difficult to count and to qualify. Analysis of current Dutch laws or proposals (especially the amendment to the Passport Act and the Act relating to Foreigners of 2000 - see *below*) show that *centralisation* is the trend in the Netherlands.

5.3.2 Current Biometric Government Application

Since 26 August 2006, all Dutch passports are issued as a biometric passport with an embedded RFID chip for storing the face scan. Two finger scans have been added since September 2009. An amendment¹⁸⁸ to the Passport Act enabling the storage of finger scans *in a central data base* on top of two finger scans on the chip in the passport itself was

¹⁸⁴ CIS (*Coördinatiegroep Informatievoorziening Strafrechtsketen*), *Protocol for establishment of identity (in law enforcement) (Protocol Identiteitsvaststelling (strafrechtketen))* ('Progis'), 3 September 2008, Directie Generaal Rechtspleging en Rechtshandhaving, the Hague, 2008.

¹⁸⁵ P. de Hert, W. Scheurs and E. Brouwer, "Machine-readable identity Documents with Biometric Data in the EU - part III - Overview of the Legal Framework", *Keesing Journal of Documents and Identity*, 2007, No. 22, pp. 23-26.

¹⁸⁶ *The Use of Privacy Enhancing Aspects of Biometrics*, de Hert and Sprokkereef, 2009.

¹⁸⁷ See Article 27 of the Dutch Data Protection Act. The so-called notification duty (*meldingsplicht*) applies to all automatic data processing, with the exception of processing falling within the decision with exemptions (*Vrijstellingbesluit*).

¹⁸⁸ First Chamber, 31.324 (R1844).

passed in 2009. The amendment to the Passport Act provides that the *public prosecutor can request access to the data in the central database 'Gemeentelijke Basisadministratie'*, under the strict rules applying to access to data in the context of a criminal investigation.

¹⁸⁹ In a recent article a Dutch prosecutor has argued that this threshold applied to prosecution access will in practice be relatively low.¹⁹⁰ The central storage provision has been adopted by Parliament, but is not yet in operation. This imminent central storage goes further than the European Passport Regulation requires, this regulation has left the decision whether or not to store passport data centrally to the national authorities. For a ruling touching on the necessity of central storage, we refer to the *Huber* case¹⁹¹ of the European Court of Justice.

Finger scans of foreigners (including other EU citizens)¹⁹² are also stored centrally in the Netherlands, that is to say: in a Foreigners' Database for the purpose of identification. The finger scans are stored to prevent identity fraud and to make the implementation of the Foreigners Act 2000 more efficiently. The finger scans are *not stored for law enforcement purposes*.

After the *Huber* case, the Commission Meijers, the Dutch Standing Committee of Experts on International Immigration, Refugee and Criminal law,¹⁹³ has suggested¹⁹⁴ that the European Court of Justice may find a swipe search of the Foreigners' Database on the basis of Article 55c Code of Criminal Procedure¹⁹⁵ unlawful. In a reply to the Dutch Senate, the

¹⁸⁹ Artikel 4b, al. 4 of the amendment states it in Dutch as follows : 'De verstrekking van biometrische kenmerken van de houder uit de reisdocumentenadministratie in de gevallen, bedoeld in het tweede lid, onder a en c, geschiedt uitsluitend aan de officier van justitie. De verstrekking vindt slechts plaats: a. ten behoeve van de vaststelling van de identiteit van een verdachte of veroordeelde voor zover in het kader van de toepassing van het strafrecht van hem biometrische kenmerken zijn genomen en er twijfel bestaat over zijn identiteit; b. in het belang van het onderzoek in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten', available at <http://parlis.nl/pdf/kamerstukken/KST121168.pdf>

¹⁹⁰ K. Hermans (2010), "Het Gebruik van Vingerafdrukken voor Opsporingdoeleinden onder de Nieuwe Paspoortwet en Artikel 8 EVRM", *NTM-NJCM-Bulletin*, jrg 35, nr 1, 35-40.

¹⁹¹ OJ C 44 21.2.2009, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:044:0005:0005:EN:PDF>

¹⁹² See Article 1(e) of the Foreigners Act 2000, available at <http://www.legislationline.org/documents/id/4680>

¹⁹³ The Standing Committee of Experts on International Immigration, Refugee and Criminal law, is an independent committee established by five non-governmental organisations: the Dutch Bar Association, the Refugee Council, the Dutch section of the International Commission of Jurists, the Dutch Centre for Immigrants/FORUM and the National Bureau against Racism (LBR). It monitors developments in the area of Justice and Home Affairs and presents its opinion to the Dutch Parliament, the European Parliament, parliaments in other Member States, the European Commission and to other public authorities and non-governmental organisations.

¹⁹⁴ The Commission Meijer has published an open letter about the Bill on identification of suspects (*'Wetsvoorstel Identiteitsvaststelling verdachten'*) on the 22nd January 2009, which is available at <http://www.commissie-meijers.nl/assets/commissiemeijers/Commentaren/2009/CM0901%20Brief%20Commissie%20Meijers%20Wetsvoorstel%20Identiteitsvaststelling%20verdachten.pdf>

¹⁹⁵ Article 55c of the Code of Criminal Procedure provides for a procedure which allows the prosecutor to access data held by other authorities under certain circumstances.

Minister of Justice has indicated that he does not think this is the case. He refers to the fact that in the proposal for the amendment to the Passport Act, Article 4a (1) stipulates that a face scan and four finger scans of every Dutch citizen are stored when he or she applies for a passport. As a result of Article 4b (4) of that amendment, the public prosecutor can request access to these data. According to the Minister, the conditions in the law which apply to a Dutch passport holder who is suspected are similar to the ones in applying to a suspect who 'is probably an alien' and 'a search request is made by the prosecutor in order to have access to data of foreigners in the database.'¹⁹⁶

An interesting legal point is here whether the Minister in fact implies that swipe searches can be held in both databases to compare the finger scans of a suspect against all scans held.

The goal of the law on Identification in the Criminal Justice Chain¹⁹⁷ is to strengthen a trustworthy identification of suspects and convicts in the criminal justice chain: Progis Protocol Identification in the Criminal Justice Chain (Progis Protocol identiteitsvaststelling in de Strafrechtketen). This Act on the Identification of Suspects, Convicts and Witnesses (*'Wet identiteitsvaststelling verdachten, veroordeelden en getuigen'*) recognizes four ways of identifying a person: a declaration, the presentation of a valid identification document, providing a face scan and finger scans. The law indicates which type of identification is required/allowed at which moment in time. The law also introduces new elements such as that the suspect needs to identify him or her self before a judge. The proposed law was passed by the second chamber of the Dutch Parliament in December 2008 and adopted by the Senate Chamber in 2010. The Progis protocol has in the meantime been tested within the criminal justice system and several changes have been made. The protocol relies heavily on the efficiency and effectiveness of biometric identification and verification.

5.3. 4 Legislation

In the Netherlands, as in many other countries, the existing data protection legislative framework governs the use of biometrics and no separate legislation has been proposed or adopted. As the data protection perspective on technology is characterised by an 'enabling logic', law has not acted as a barrier to the diffusion of biometric technologies. Thus, data protection legislation makes existing processing practices transparent, and does not

¹⁹⁶ *Memorie van Antwoord 31436*, 17 March 2009, p. 11, available at <http://www.dnasporen.nl/docs/wetregelgeving/KST128925.pdf>. The Minister stated it as follows: 'These conditions are materially similar to the conditions under which the fingerprints of foreigners for the purpose of determining the identity of a suspected foreigner (see Article 55c, second and third paragraph, Code of Criminal Procedure) and the detection and prosecution of criminal offenses (see my letter of November 12, 2007) are consulted. Therefore, I believe, contrary to the Commission Meijers, that there is no reason to doubt whether the Court would deem it acceptable that the fingerprints that have been taken from a suspect on the basis of Article 55c, second and third paragraph, Code of Criminal Procedure are compared with the fingerprints that have been processed in the context of the "Basisvoorziening Vreemdelingen", if the suspect is probably a foreigner' (free translation).

¹⁹⁷ http://www.eerstekamer.nl/behandeling/20081202/gewijzigd_voorstel_van_wet_2/f=y.pdf

prohibit them as a rule.¹⁹⁸ In other words, Dutch data protection regulations create a legal framework based upon the assumption that the processing of personal data is allowed and legal in principle.¹⁹⁹ Therefore, ownership of individuals regarding their data is not recognised, but individual controlling rights are granted instead.

The legal framework for data protection in general in the Netherlands consists of Article 10 of the Dutch Constitution, Directive 95/46/EC, the Dutch Data Protection Act ('*Wet Bescherming Persoonsgegevens*')²⁰⁰, and a number of other specialized laws and regulations such as the Medical Treatment Agreement Act ('*Wet op de Geneeskundige behandelingsovereenkomst*')²⁰¹, the Database Act ('*Databankenwet*'), the Municipal Database Personal Files Act ('*de Wet Gemeentelijke Basisadministratie*')²⁰², the Police Files Act ('*Wet Politie registers*')²⁰³, Foreigners Act ('*Vreemdelingenwet 2000*')²⁰⁴ and the Telecommunications Act ('*Telecommunicatie Wet*').²⁰⁵

The Data Protection Act is applicable to the collection and processing of personal data and also applies to the processing of biometric data.²⁰⁶ The Act does not contain specific provisions that mention biometric data as such. Nevertheless, there has been hardly any discussion about whether, or under which conditions, biometric data should be considered personal data. In 2007, a report called *First Phase Evaluation of the Data Protection Act*, presented an analysis of the obstacles in the implementation and application of the Data Protection Act.²⁰⁷ One of its conclusions was that 'the vagueness of the concept of personal data implies obscurity on the scope of the act and this leads to

¹⁹⁸ There are exceptions. Some sections of the data protection regime provide for a prohibition of processing (e.g. sensitive data, secretly collected personal data) in which case such processing operations actually fall under a privacy or opacity ruling.

¹⁹⁹ An outright processing ban effectively applies only to special categories of sensitive personal data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. On the limitations of the data protection approach see also A. Sprokkereef(2008), 'Data Protection and the Use of Biometric Data in the EU', S. Fischer Huebner, P. Duquenoy, A. Zaccato, L. Martucci (eds.), *The Future of Identity in the Information Society*, IFIP (International Federation for Information Processing), 2008, Volume 262, Boston Springer, pp 277-284.

²⁰⁰ The Dutch Personal Data Protection Act of 2001, last amended in 2002, available at http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml

²⁰¹ http://wetten.overheid.nl/BWBR0007021/geldigheidsdatum_31-03-2009

²⁰² http://wetten.overheid.nl/BWBR0006723/geldigheidsdatum_31-03-2009

²⁰³ http://wetten.overheid.nl/BWBR0010477/geldigheidsdatum_31-03-2009

²⁰⁴ http://wetten.overheid.nl/BWBR0011823/geldigheidsdatum_31-03-2009 ; This Act is also available in English at <http://www.legislationline.org/documents/id/4680>

²⁰⁵ http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_31-03-2009.

²⁰⁶ For one of the first Dutch attempts to provide an oversight of all laws that govern particular aspects of biometrics: S. Artz and van Blarkom, 'Beveiliging van persoonsgegevens: de WPB. Privacy en Biometrie: een technisch vraagstuk?', *Jaarboek Fraudebestrijding*, 2002.

²⁰⁷ G.J Zwenne, A.W. Duthker, M. Groothuis, H. Kielman, W. Koelewijn en L. Mommers, *Eerste Fase Evaluatie Wet Bescherming Persoonsgegevens: Literatuuronderzoek en Knelpunt Analyse*, eLaw@Leiden/WODS, 2007 ('*Eerste Fase Evaluatie*').

divergent interpretations'.²⁰⁸ It can therefore not be excluded that *encrypted biometric data will in certain instances not be regarded as personal data under Dutch law*. There is, however, no case law at all in this field yet. It is remarkable that the 211 pages report does not mention biometrics once. As the report is based on a literature and case law study only²⁰⁹, this just reflects the fact that no conflicts or obstacles in the area of biometric data handling have arisen so far.

The second part of the evaluation report (the second phase evaluation) will be based on empirical research and might throw more light on the application of Dutch Data Protection Act to biometric data handling. Based on our own study²¹⁰ and the general conclusions of the *First Phase Evaluation of the Data Protection Act* report, we are making an informed guess in stating that the use of biometrics takes place against a background of lack of knowledge and information provision. One of the conclusions of the report is that 'self regulation within the scope of the Data Protection Act leaves much to be desired'.²¹¹ The final conclusion of the report is that many rights and obligations of controllers and persons involved that arise from the Data Protection Act are not effectively exercised through a lack of familiarity with these rights.²¹² Thus, one of the core objectives of the Data Protection Act, *to increase the transparency of data processing* through the granting of rights and obligations and the introduction of a regulatory authority, has not been fully achieved yet.

5.3.5 The National Data Protection Authority on Biometrics

In the Netherlands it is not mandatory to request an opinion on or an authorization from the national data protection authority for the processing of biometric data. A notification of the use of a biometric application with the DPA is all that is required to get a new biometric application started. Normally, the DPA does not take further steps after it receives the notification of the processing of biometric data.²¹³ In principle, the notification to the DPA does not imply an approval. To the contrary, the notification allows the authority to react if this is needed. In practice, and due to *staff constraints*, this seldom happens, however. As it is not required that the processor or controller waits for a 'green light', the controller can start the processing straight after notification. Thus, in practice the role of the DPA has been to receive notifications, to make an administrative check on them and to place all notifications on a register accessible

²⁰⁸ *Eerste Fase Evaluatie*, p. 210.

²⁰⁹ See *Eerste Fase Evaluatie*, p 5.

²¹⁰ *The Use of Privacy Enhancing Aspects of Biometrics* 2009.

²¹¹ *Eerste Fase Evaluatie*, p. 211. According to the authors, especially further interpretation of substantive standards through self-regulation has only been realized to a restricted extent.

²¹² *Eerste Fase Evaluatie*, p. 211.

²¹³ See also *The Use of Privacy Enhancing Aspects of Biometrics*.

through its website.²¹⁴ A few organizations have asked the DPA to issue a preliminary opinion. In general, the Dutch DPA's activities are of a re-active nature.²¹⁵ Concerning the semi public or private use of biometric applications, the main supervisory activity of the DPA has been the publication of three preliminary (non-binding) opinions. The first relates to an access control system with the use of a biometric disco pass²¹⁶ In 2001, a producer requested the DPA an opinion on an access control system named 'VIS 2000'.²¹⁷ This biometric system was designed for use by sport centres, social clubs or similar establishments. Apart from organising access control, the system served marketing and management purposes and allowed keeping a 'black list' of customers who had violated the rules. The VIS 2000 stored the templates of the fingerprint and the face. The templates of the face were stored in a central database, combined with the membership card number. The DPA stated in its opinion that the use of biometric data for access control purposes is far reaching. It should be evaluated whether the use of biometric data is in proportion with this purpose. To this end, the DPA checked the collection and use of the biometric data against several obligations of the Data Protection Act. In this opinion, the DPA explicitly recognizes the possibility of the algorithm used to reconstruct the face of the original scanned facial image from the template. This reverse engineering of the templates was one of the main functionalities of VIS 2000 in identifying violators. This technical feature, however, has important consequences. First, it should be noted that the face scan might well contain information about race, which shall in principle not be processed. The Dutch Data Protection Act contains an explicit exception to this prohibition of processing of this information, in particular, when such processing is used for the identification of the person and to the extent that this is necessary for this purpose. On the one hand, the DPA concluded it was inevitable that use is made of templates of the face (containing information about race) for the identification of troublemakers.²¹⁸ The DPA concluded its opinion with several recommendations, including conditions for storage and security (encryption of templates and membership card numbers) and for the operation of the biometric system. This opinion of the Dutch DPA is different from the evaluation, comments and conclusion of the Belgian DPA with

²¹⁴ See www.cbp.nl.

²¹⁵ For a comparison between for example Belgium and the Netherlands see also E. Kindt and J. Dumortier, 'Biometrie als Herkenning- of Identificatiemiddel', *Computerrecht* 2008, p. 132 *et seq.* and P. De Hert and A. Sprokkereef, 'Biometrie en Recht in Nederland', *Computerrecht*, 2008, pp. 301-302.

²¹⁶ CBP (before 'Registratiekamer'), *Biometrisch toegangscontrole systeem VIS 2000*, 19 March 2001 ('*discopas opinion*'), available at www.cpbweb.nl.

²¹⁷ About this opinion, see also E. Kindt, '3.2.2. Situation in some selected countries. The Netherlands', in FIDIS deliverable *D3.10 Biometrics in Identity Management*, E. Kindt and L. Müller (eds), p. 45 *et seq.*, available at www.fidis.net

²¹⁸ As stated above, the DPA *did not make a proportionality test about the use of biometric data*, and the opinion therefore indicates that a necessity test to use information about race should be regarded as sufficient for the purpose.

regard to a similar system. The Belgian DPA reported in its annual report of 2005 that it rendered a negative opinion on a similar system. It considered the use of biometric characteristics for access control for a dancing club not proportionate with such purpose.²¹⁹ More particular, the Belgian DPA found the use of biometrics for identification purposes disproportionate and entailing risks for the privacy of the visitors.

The second opinion relates to changes to the Passport Act involving the introduction of biometrics.²²⁰ On 19th September 2001, the Dutch Home Office Minister requested the DPA's advice on some new paragraphs proposed to Article 3 of the passport law. On examination of the provisions, the DPA concluded that the new passport law would allow biometric data to be stored in the travel document administration of the appropriate authorities. The DPA pointed out that there were not enough arguments to support the necessity of the measure. On the basis of the current arguments, the DPA rejected the need for such a measure. It also stated that even if these grounds were to be put forward, the Passport Act would still need to be based on the purpose limitation principle, whilst in the current wording the purpose was open ended.

In a second advice of 30 March 2007, this argument was repeated, and the DPA *argued against (de-)central storage, warning for the effect of 'function creep'*.²²¹

A strong proponent of storage of original biometric data is Grijpink who argues that decentralized storage of four (instead of two in the passport only) finger scans in the local data base of a Dutch municipality is a very powerful way to prevent large scale identity fraud with biometrics in passports.²²² In the absence of a database, the biometrics of an individual who claims to be the victim of identity fraud cannot be checked against original finger scans stored, and the perpetrator can easily go undetected. According to Grijpink, in the case of *small scale, private or semi public applications, this argument does not hold*, because the impact of identity fraud is not so profound and proportionality becomes a more important issue. In smaller scale applications, it is also possible to detect or prevent fraud through other means.

The third opinion was issued in 2004 on the use of face recognition and the use of biometrics for access control to public events, combined with use for police investigations²²³

In the case, the data protection authority found a strong link between access control and identification: the templates were stored in an event data base and the use of the smart

²¹⁹ See E. Kindt, *I.c., Datenschutz and Datensicherheit (DuD)*, 2007, N° 31, pp. 166-170.

²²⁰ CBP, *Wijziging Paspoortwet z2001-1368* (invoering biometrie), 16 October 2001.

²²¹ CBP, *Wijziging Paspoortwet advies z2007-00010* (invoering biometrie), 30 maart 2007, 5 (cbpweb.nl)

²²² J. Grijpink, 'Biometrie, Veiligheid en Privacy', *Privacy en Informatie* 2008, Vol 11, pp. 10-14; J. Grijpink, 'Two Barriers to Realizing the Benefits of Biometrics', *Computer Law and Security Report* 2005, Vol. 21(3), 249-256; J. Grijpink, 'Biometrics and Privacy', *Computer Law and Security Report* 2001, Vol. 17(No. 3), pp. 154-160.

²²³ CBP, *Vragen over de inzet gezichtsherkenning z2003-1529*, 3 February 2004.

card is not restricted to access control. Therefore *the objectives* of the access control system needed careful examination and specification, especially when visitors have no other option than using the system. The data protection authority concluded that when the detection of a violator *depends only to a limited extent on the templates* stored on the event data base, then the use of the system threatens to become *disproportional*. If the use of the system does not really produce more benefit than the already existing instruments to detect violators, then the concept contains unnecessary processing of data. The DPA confirmed that unnecessary processing of data is illegal.²²⁴

In the conclusion, the third DPA opinion introduces the basic condition that it needs to be proven that the use of face recognition technology increases safety in a proportional manner. The key sentence in the opinion is the following:

“When the introduction of the system, in view of all the instruments already available, does not provide additional value, the concept entails unnecessary processing of data”.²²⁵

6 Shortcomings of European Data Protection

There are, however, many shortcomings to European data protection that generate problems with almost every new technological development that is considered under this framework. Problems can be identified that relate to the enabling logic of data protection, problems that relate to the duty to secure personal data, problems that relate to the character of biometric data and the technologies enabling the data to be read, and problems that relate to the abstract, ethical vague nature and limited scope of the EU competencies.

Although the Directive was almost designed for the Information Society, application of the Directive to problems occurring through the use of the Internet remained contested up until the famous *Lindqvist* Judgement of the Court of Justice.²²⁶

Questions with regard to the application of the Directive on processing of sound and image data have been reported in the first report on the implementation of the Data Protection Directive published by the European Commission of the European Communities.²²⁷ Although the central message of the report was that there was no reason to panic and that the Data Protection Directive could handle the new

²²⁴ See the full opinion on a detailed test of the concept of data processing: CBP , 27 May 2004, z2003-1529.

²²⁵ See also section 6.1.2. of the fore mentioned opinion of the DPA.

²²⁶ Court of Justice, *Bodil Lindqvist v. Sweden*, Judgement of 6 November 2003 (No. C101/01), <http://www.europa.eu.int>,

²²⁷ Commission of the European Communities, *First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels, 15.5.2003, COM(2003) 265 final, (27p.), 20

evolutions,²²⁸ several crucial problems of interpretation remain with the application of the general rules of data protection,²²⁹ and that additional rules and guarantees are demanded by some for questions such as CCTV and biometrics.²³⁰ On data processing the review reported that it was “hard to obtain accurate or complete information about its compliance with the law”. However, on the basis of anecdotal information three interrelated problems were identified: “under-resourced enforcement”, “patchy compliance by data controllers” and “low level of knowledge about their rights among data subjects”. The first report (five years after implementation) turned out to be the only review so far²³¹ and there have been no proposals to improve the Directive or any evidence that the situation has improved.

In one of the first studies on biometrics, Prins argued that the Directive *does not* apply to templates on smart cards, because this kind of data is not about *identified or identifiable persons*.²³² On closer scrutiny this interpretation cannot be upheld. The Preamble

²²⁸ "The Commission has based this review on a study carried out by an external contractor to analyze the situation in the Member States and on contributions from the Member States themselves and the national supervisory authorities. The information received shows that the processing of sound and image data falls within the scope of all national laws implementing the Directive and that the application of the Directive to these categories of processing has not been particularly problematic".

²²⁹ "There is in addition a number of legal and practical issues resulting from the implementation of the Directive in the Member States as regards sound and image data that create some uncertainty for operators called on to comply with the legislation and for individuals entitled to exercise their data protection rights. There are for instance uncertainties as regards the definitions of the Directive, for example, to what extent an isolated image or a finger print can be considered personal data in those cases where the data controller is unable or extremely unlikely to identify an individual; or whether simple monitoring constitutes a processing operation or how to achieve a reasonable interpretation of the concept of sensitive data.

²³⁰ Comp. "During the Directive's preparation, some people were concerned that it might not be able to cope with future technological developments. The extent of such technological developments was uncertain, but there was concern that a text drafted mainly with text processing in mind could encounter difficulties when applied to the processing of sound and image data. For this reason, Article 33 contains a specific reference to sound and image data (...). No Member State or other contributor has proposed modifications to the Directive in this regard.

²³¹ See *Statewatch*, 2008, 42.

²³² Prins, 1998, 161-162: "Of prime importance is the criterion set in article 2 (a): the processing must concern data about *identified or identifiable persons*. Preamble 26 stipulates in this respect that in order to determine whether a person is identifiable, all justifiable means can be undertaken to identify a particular person, which is a rather broad definition. As mentioned in paragraph 2, the templates containing the biometrical data can be stored and used off-line as well as on-line. Organisations could opt for central storage in a large database (on-line) or storage on a smart card (off-line). When stored in a database, the biometrical information is often connected to other personal data, such as names or addresses of the individuals. This need not be the case with storage on a smart card. Here, the smart card could merely contain the biometrical data, thus revealing no information that may link the data to a specific individual. This type of use allows for the verification of individuals (*e.g.* this person leaving the building is the same as the one who entered the building, without the necessity of knowing *who* this person is), whereas the on-line use allows for the identification of an individual (*e.g.* used in situations where the identity of the person is essential). Turning to the implications of the use of the different systems under the personal data protection rules, it appears that the use of an off-line system is not

advances a broad interpretation of the notion of 'identifiable'.²³³ Even when biometrics are used off-line (e.g. on a smart card) it is always possible with the help of the processor of the smart card to identify a smart card holder, hence the Directive applies. Of course one could argue that these kinds of interpretation problems can be overcome by the work of judges, in particular the Court of Justice, having the authority to interpret the law. However, the many hesitations of the Court of Justice in *Lindqvist* and the small deviations of the regular interpretation of the Directive given by data protection experts, such as the Working Group 29,²³⁴ leave many legal issues unsettled.

A second problem has to do with so called sensitive data (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual preference).²³⁵ Article 8 of the Directive contains a prohibitive rule with regard to this kind of data. The core of the underlying motive is that the processing of these sensitive data bears a supplementary risk of discrimination.²³⁶ Derogation is only possible in strictly defined circumstances, for example for reasons of national security and when there is explicit consent.²³⁷ In certain situations the use of biometrical data could imply use of sensitive personal data. Blood or DNA data belong to the category of sensitive data since they somehow concern the health of natural persons.²³⁸ Also, when opting for fingerprint techniques or face recognition techniques, racial or ethnic origin can be revealed.²³⁹

These statements are open to interpretation. When exactly do blood samples fall within the category of sensitive data? Do templates as such not qualify as sensitive data because

subject to these rules. The processing does not concern data about *identified or identifiable persons* and in the majority of the situations no means allow for the identification of a particular person".

²³³ Directive 95/46/EC, Preamble, § 26: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible".

²³⁴ P. De Hert. & W. Schreurs, 'De bescherming van persoonsgegevens op het Internet: nuttige verduidelijking door de rechtspraak' [Protection of data on the Internet: Useful interpretations given by the Court], annotation of *Bodil Lindqvist v. Zweden, Auteur&Media*, 2004/2, 127-138 (with French summary)

²³⁵ Directive 95/46/EC, Article 8.1.: " Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".

²³⁶ Directive 95/46/EC, Preamble, § 33. See also: Alonso Blas 2003 *I.c.*, 504.

²³⁷ When falling under the scope of the said Article, biometrics will have to meet additional legal demands have to be met, among which explicit consent of the data subject (article 8 Directive) following from the principle rule prohibiting the processing sensitive data.

²³⁸ Alonso Blas 2003, *I.c.*, 504.

²³⁹ Prins, 1998., 162.

the digital data of the template cannot be translated back into the biometrical data? Thus, a template as such never constitutes sensitive data. However, in situations where the original scanned image is not destroyed and kept in a database, the storage of the relevant data must meet the specific conditions set by Article 8 of the Directive.²⁴⁰ These deductions have to be confronted with scientific expertise, especially the assumption that templates are irrevocable.²⁴¹ Also it is important to understand in which situations sensitive personal data are processed by which technology. It is tempting to suggest that only biometric technologies using physical characteristics process sensitive data, while technologies using behavioural characteristics do not. However, voice recognition is both biological and behavioural biometrics and could as well give information relating to racial or ethnic origin and health. On the other hand, it might well be that judges and policy makers do not regard biometrical data as sensitive data as long as the purpose of the processing is not to identify sensible data. The Belgian Data Protection Authority in its recommendations with regard to visual data has defended this position.²⁴² The Commission has taken the view that pictures of people taken for security purposes do not fall within the category of sensible data, because of the purpose of security cameras.²⁴³

5.1 Enabling Without Limits

A more fundamental critique with regard to data protection is directed against the business- and government-friendly (enabling) logic behind the framework. In standard procedures in the Netherlands for example, a notification of the use of a biometric application with the Data Protection Authority is all that is required to get processing of data going. Formally, a notification to the local authority does not imply a formal 'go'. On the contrary, the notification allows the authority to react if this is needed. In practice and due to staff constraints²⁴⁴ this seldom happens. It is also not required that the processor or controller waits for a 'green light'. The processing can be started once the notification is done.

The strength of data protection, -its ability to deal with new technologies-, can also be its weakness when it creates a situation wherein market forces and dominant powers do the legislator's work. When the latter then finally turns his attention to the problem, he will have to face the fact that once technology is accepted, the more difficult it will be to limit

²⁴⁰ Prins, 1998, *I.c.*, 162.

²⁴¹ Comp. with Institute For Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview, o.c.*, 47 suggesting that in the future this may change. See also EBF 2007.

²⁴² For a detailed analysis of the legal approach to biometrics in Belgium see: Kindt and Dumortier, (forthcoming).

²⁴³ See De Hert et al 1996.

²⁴⁴ See implementation report supra.

it later on.²⁴⁵ When technologies are new, or are used in newer ways such as the application of satellite technology to cellular phones, their uses are easier to modify and their consequences are easier to control. The use of security and identification technology in the form of biometrics, detectors, surveillance equipment, and advanced forms of access control are in the early stages of implementation. In we wish to assess the unintended consequences of these developments, now is the time to do so.²⁴⁶ Although small privacy impact assessments have been carried out in the EU, this is generally regarded as an underdeveloped instrument preventing smart regulation.²⁴⁷ The European Data Protection Supervisor has many times called for privacy impact assessments before new European legislation relating to biometric applications were to be adopted. Elsewhere we have argued the case for a societal impact assessment.²⁴⁸

5.2 'Secondary use' & 'Proportionality' vs. Diffusion Effect

The sheer wordings of the data protection principles (the fairness principle, the openness principle and the accountability principle, the individual participation principle, ...) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice. We already observed that data protection regulations created a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal. The lack of normative rules in data protection weakens the potential of the instrument to deal with on its own strength with new developments. Unfortunately, this problem of guidance with data protection is often underplayed. Fair information practice norms do not provide adequate criteria for determining whether a given means of data collection is ethically acceptable. Basic notions in the Directive such as 'fair processing' and 'legitimate grounds' are not independent notions. Something is 'fair in the light of'. Certain acts are legitimate in 'the perspective of'. From an economic perspective, most processing done by business is legitimate. From a security perspective, most processing of data done by police or intelligence forces is legitimate. This explains why one of the most normative provisions in the Directive, viz. Article 6,1,²⁴⁹ is by itself unable to address important questions, such as: 'When is a processing

²⁴⁵ Anton Alterman, 2003 *I.c.*, 149.

²⁴⁶ Casella 2003, 92. This author adds: "Too little is known about the consequences of the uncontrolled uses of these technologies, yet most policymakers support them due to their allure and short-term promises of safety. If society becomes safer, if it becomes more difficult to smuggle weapons into schools, or if violence decreases, advocates of these technologies will claim that these are their *intended* consequences. However, if public and private institutions begin to resemble prisons, if new generations begin to accept unmitigated surveillance as a natural part of life, if people's civil rights become gradually revoked, or if people lose opportunities to develop human relationships, such consequences must be viewed as *intended* as well".

²⁴⁷ Cunningham and Grabosky, 2003.

²⁴⁸ Sprokkereef, 2008.

²⁴⁹ Directive 95/46/EC, Article 6.1.: "Member States shall provide that personal data must be:

proportional?', 'How many functions should a smart card have'. For what purposes can an existing biometrical database be used? It is not always reassuring to read in the subsequent paragraph that "It shall be for the controller to ensure that paragraph 1 is complied with" (Article 6.2.). It is moreover troublesome that many Member States have implemented the Directive without further specifications. Take for instance Article 6 1. (b): data must be collected for specified, explicit and legitimate purposes. Clear enough: once the data subject is informed about the processing, he knows what happens with his data. However, the same provision allows secondary use: collected data can be 'further processed in a way incompatible with those purposes'.²⁵⁰ Does the data subject have a right to be informed of this secondary use? This is where data protection meets freedom of information. Under which circumstance does or does the data subject not have a right to know what data is held on him or her? Should he or she be able to have biometric data corrected or even deleted? In other words: how can a government promote both privacy and openness? The interface between data protection and freedom of information is very complex and I will examine this further in chapter three. Here it will suffice to note that if the legislator wants to address the risk of a 'diffusion' effect of biometric technologies from security to non-security applications and of its future pervasive use in everyday life, additional regulation is needed. Generally speaking it is enough for the current application of Article 6 that some transparency is created towards the data subject. The more transparency is given about the (secondary) use, the more consent is obtained²⁵¹ the more *finalities* or purposes can be given to biometrical technologies and the more *proportional*.

-
- (a) processed fairly and lawfully;
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use".

²⁵⁰ This exception is again implemented in many Member States without additional safeguards.

²⁵¹ We recall that consent is one of the grounds defined in Article 7 of the European Directive that make processing 'legitimate' in the sense of the Directive. Even within the category of sensitive data protected by Article 8 'explicit consent of the data subject' is mentioned as one of the possible legitimate grounds. Blas rightly observes that the consent obtained by data law enforcement authorities when collecting or processing data is often not freely obtained: "A person who is considered a suspect of a crime or offence is not totally free to decide whether or not to co-operate with the forensic researchers. Caution is therefore necessary when using consent in this context" (Alonso Blas, 2003 *l.c.*, 505).

Within the current data protection framework there is no obstacle for processors and controllers choosing for on-line biometrics rather than off-line biometrics or choosing for the more intrusive forms of central storage.

6.3 Second Generation Biometric Data: From Visible to Invisible data Collection

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. So, let us assume first that the individual subject knows that he is subject to biometric processing of the second generation. There is then mainly a tension between the processing of second generation biometric data and the individual participation principle. How to check and verify if the biometrical data are still accurate? The obvious risk that the systems (and not only personal data) may be used by other persons and for other purposes than foreseen is difficult to minimize, without the traditional possibilities for individual participation. How to exercise the right to have the data corrected or the right to object to certain types of data processing? Does an individual for example know that the biometrical identifiers are still working? Here 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 pales into insignificance when assessing the applicability of data protection law in situations where the subject is unaware of the invisible data collection. Therefore, our main and immediate 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. First, 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 rights and obligations of the EC Directive 95/46.²⁵² The Directive may allow statistical processing or profiling of personal data, once the data are made anonymous.

Recital 26 states “whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.” Article 6.1.b is very specific: “further processing of the data for historical, statistical or scientific purposes is not considered as incompatible provided that appropriate safeguards are provided by the Member States whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual.”

Article 15 of the Data Protection Directive principally prohibits that a person is subject to automated decisions which produce legal effects concerning him, or significantly affects him, and which are based solely on automated processing of data intended to evaluate

²⁵² Hildebrandt and Backhouse 2008; Hildebrandt and Gutwirth 2008

certain personal aspects relating to him. This Article thus gives individuals the right to object to decisions affecting them when decisions are made solely on their profiles.²⁵³ This provision however, is accompanied by numerous exceptions that do not set strong and clear-cut limits to targeted profiling actions. The results of data profiling can be applied afterwards to data subjects without them knowing that the profiles are applied to them, for example: people can be individually stopped or checked at a border control because they fall under a certain profile. How is it guaranteed that the data subject is informed that such automated individual decisions are applied to him? Are there any guarantees that the data subject can exercise the right to obtain from the controller knowledge of the logic involved in such automatic processing operations? Will all authorised agents acting upon these automated decisions ‘know’ this logic involved and be able to communicate this logic to the data subject? Profiling should not only be addressed with a mix of modes of regulation, but this mix must also construct an appropriate articulation of opacity and transparency tools.

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. In fact, existing European legal mechanisms cannot guarantee effective protection against profiling. This has already led to a call for widening the protection currently granted through the regulation of ‘unsolicited communications’ via the new notion of ‘unsolicited adjustments’. The notion of ‘unsolicited adjustments’ would close a legal loophole allowing a situation in which objects that seemingly have a neutral guiding function, in practice secretly track individuals to surreptitiously adapt their performance based on undisclosed criteria.²⁵⁴ Similarly, gaps in current data protection, in the case of second generation biometrics applied in real life situations, can lead to forms of profiling that leave some of the rights for individual, such as the right to have data corrected, or the right of access to the data, unprotected. Approaching new phenomena such as profiling with heavy prohibitions may block progress or lead to a situation where the prohibitions are not respected.²⁵⁵ There does not need to be a choice between the opacity approach of data protection (prescriptive rules) and a data transparency approach (making data handling visible and data handlers accountable). In the regulation of profiling, opacity and transparency tools can each have their own role to play. In a normative weighing of privacy and other interests, some intrusions will turn out just to be too threatening for fundamental rights whilst others will be accepted and submitted to the legal conditions of transparency and accountability.

²⁵³ Gutwirth and De Hert, 2008, 283.

²⁵⁴ Gonzalez Fuster G. et al, (2010), “From unsolicited communications to unsolicited Adjustments. Redefining a key mechanism for Data Protection” in : S. Gutwirth, Y. Poulet and P. De Hert, *Data Protection in a Profiled World*, Springer, Dordrecht.

²⁵⁵ Gutwirth and De Hert, 2008, 284.

7 Recommendations

The existing legal framework for biometrics is in essence an ‘enabling legal environment’ regulating the use of biometrics but in fact lacking normative content.²⁵⁶ For that reason, more specific rules are needed which prohibit use where there are disproportionate power balances.²⁵⁷ Such legislative initiatives have to be sufficiently precise. Regulation which provides for the use of biometrics ‘for security purposes only’ is superfluous.²⁵⁸ Most of the analysis and the country reports mentioned in this deliverable refer to opinions or positions of institutes or authorities (in many cases of DPAs and the EDPS) which have studied biometrics. DPAs and the EDPS have clearly indicated that there are numerous risks of central databases with biometric data. They opt for a clear rejection, to a greater or to a lesser extent, of the central storage of biometric data in databases, because of the risks.²⁵⁹ These risks increase if the databases contain biometric characteristics which leave traces or can be collected without the knowledge of data subjects, such as fingerprint, face, voice, but also DNA.²⁶⁰ But only few countries, such as Germany, have enacted laws which forbid the establishment of central biometric databases. In that case, such legislation is mostly in relation with a specific biometric application, such as the epassport.

A general prohibition on the collection and use of biometric characteristics and/or technologies without the knowledge of the individual is recommended in order to avoid that biometric characteristics which leave traces are abused (e.g., use for identification, linking or surveillance, but also for abusing the sample). Such prohibition is needed to protect the fundamental rights and freedoms²⁶¹ and to increase public confidence. This

²⁵⁶ DG JRC and IPTS, *Biometrics at the Frontiers : Assessing the Impact on Society*, Sevilla, January 2005.

²⁵⁷ DG JRC and IPTS, *o.c.*, p. 15.

²⁵⁸ Compare, for example, with the legislation in Slovenia which regulates the use of biometrics but only in a general way.

²⁵⁹ The European Parliament has also before already pleaded in its legislative resolution of 2 December 2004 on the proposed Regulation 2252/2004 for forbidding the creation of a central database of European Union passports and travel documents containing biometric and other data (see proposed Amendment 5). See European Parliament legislative resolution on the 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), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2004-0073+0+DOC+PDF+V0//EN> Furthermore, the risks and fears for central databases and its misuse is also an important factor of (dis)trust of the citizens. See in that regard, Backhouse, J. and Halperin, R., D.4.12 ‘A qualitative comparative analysis of citizens’ perception of eIDs and interoperability’, Fidis, www.fidis.net, May 2009.

²⁶⁰ In the light of new cryptographic measures for template protection, including a user specific secret as part of the verification method, this may need to be re-evaluated in specific cases of modern biometric systems.

²⁶¹ Compare with ECHR, *Peck v. U.K.*

prohibition should apply to the private and public sector data controllers, such as cities or communes, equally.²⁶²

Legislation or regulation shall also address the need for transparency in biometric systems. This shall be done by imposing an information obligation upon data controllers which is more extensive than the general information obligation of Directive 95/46/EC and which is specific with regard to the functioning of biometric systems. Legislation could require the mentioning of the identification or verification functionality of the system and clarification as to whether or not the data are stored in a central database. Multi-layered information is an option and could provide the data subject with more insight into the functioning of the system.

Regulation shall also address the errors and technical failures of biometric systems. These errors and failures, which are inherent to biometric recognition systems, will confront individuals with the limited functioning of the system. The technical aspects of the functioning of biometric systems have been described in detail in Fidis deliverable 3.10²⁶³, revealing how the physical measurement step of biometric processing systems is intrinsically error prone.

The legal framework shall hence explicitly acknowledge that biometric systems are never 100% certain and shall not disregard the errors and failures of biometric systems. Information about the error rates should be made available to the data subjects.²⁶⁴ In addition, the rights of the data subjects in case of failure shall be determined. Such rights could include (i) the right for immediate second review, at no cost and (ii) the right to use an alternative system.²⁶⁵ Furthermore, the burden of proof should be on the data controller to prove that the data subject is not the person whose identity has been verified and not on the data subject who has to prove his or her identity through a (sometimes failing) biometric system.

If human beings are obliged or requested to submit themselves to a biometric system, such system shall not dominate, but shall be at the service of the human beings. As the Project Group on Data Protection (CJ-PD) under the aegis of the European Committee on Legal Co-operation (CDCJ) also concluded in 2005, biometrics should not be chosen for the sole sake of convenience, as human dignity and equality might be affected by the use

²⁶² Such prohibition would in our view also exclude the use of face recognition technology in relation with cameras already installed. A clear legislative provision in this matter however should regulate this issue.

²⁶³ www.fidis.net

²⁶⁴ Error rates quoted by vendors are often very unreliable. The error rates should therefore be measured by an independent third party in a live test prior to full scale deployment.

²⁶⁵ An obligation for the controller to address the failure of systems, for example for Type II access control models, is for example foreseen in the Unique Authorization N° 008 of the CNIL.

of biometrics.²⁶⁶ Socio-cultural aspects and possible reluctance towards the instrumental use of the human body, should be taken into account.²⁶⁷

Moreover, the legal framework has to take the errors and failures of biometric systems in various ways into account. One possibility is to regulate the technical requirements of systems to be used for specific applications, for example by providing minimum requirements. Another route would be the setting up of a certification scheme for specific biometric systems.²⁶⁸

Finally, procedures 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 any system's performance is recommendable.

²⁶⁶ Project Group on Data Protection (CJ-PD) under the aegis of the European Committee on Legal Co-operation (CDCJ) (2005), Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data.

²⁶⁷ In the Netherlands, several cases are pending re: the Passport Act. Some individuals have started proceedings against the Dutch State on ethical grounds: see Böhre, V, 2010.

²⁶⁸ The use of certification labels is to some extent already practised in some countries, such as in Germany, for products in general and was also proposed for biometric applications in the Netherlands in the *At Face Value report* of 1999.

8. Recent Material for Further Reading

Article 29 Data Protection Working Party and Working Party on Police and Justice, *Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 December 2009.

Böhre, V. (2010), *Happy Landings: Het Biometrische Paspoort als Zwarte Doos (The Biometric Passport As A Black Box)*, Verkennende Studie voor het Rapport iOverheid, WWR (Dutch Scientific Council for Government Policy), the Hague, Webpublication Nr 46.

Bundesamt für Sicherheit in der Informationstechnik (2010), *Technische Richtlinie TR-03127: Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel*, Version 1.10, 31. March, Bonn.

Commission of the European Communities (2007), *Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, COM(2007) 619 final, Brussels, 18 October 2007, pp. 1-8.

Commission of the European Communities (2009), *Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No[.../...]* COM(2009) 342 final, 10 September 2009.

Commission of the European Communities (2008), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Commission of the European Communities (2009), Communication from the Commission to the European Parliament and the Council, An Area of freedom, security and justice serving the citizen* COM(2009)262/4, 25 November 2009.

Council of the European Union (2009), *The Stockholm Programme – An open and secure Europe serving the citizen*, 14449/09 Brussels, October 2009. Also at http://www.se2009.eu/en/the_presidency/about_the_eu/justice_and_home_affairs/

Council Conclusions on an Information Management Strategy for EU internal security, 2979th Justice and Home Affairs Council meeting, Brussels, 30 November 2009.

De Hert, P. & R. Bellanova (2009), *Data protection in the AFSJ: A system still to be fully developed? Briefing for LIBE committee of the European Parliament*, March, PE 410.692.

ENISA, *ENISA REPORT on the State of pan-European eID initiatives*, January 2009.

European Commission, Joint Research Centre (2005), *Biometrics at the Frontiers: Assessing the Impact on Society*, EUR21585.

European Court of Human Rights (2008), *Judgment of the Court (Grand Chamber) of 4 December 2008 Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04), Retention of fingerprints and DNA samples of former suspects even when no guilt has been established or when the investigation has been discontinued*, Strasbourg, 4 December 2008, pp 1-38.

European Court of Human Rights (2008), *Case of MANKA - Germany (No 23210/04) Collection of personal identification data for police records following the discontinuance of criminal investigation: communicated*. Information Note on the Case – Law of the Court. Article 6,2, Article 8 of the Convention, January 2008, No. 104, p. 19, at <http://www.echr.coe.int/NR/rdonlyres/797BA549-C2A0-4F29-85E6-E8585AE48A0E/0/Example104.pdf>.

European Data Protection Supervisor (EDPS) (2009), Press Release on *ePrivacy Directive close to enactment: improvements on security breach, cookies and enforcement, and more to come*, 9 November 2009.

EDPS (2010), The Strategic Context and the Role of Data Protection Authorities in the Debate on the Future of Privacy, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04029_Speech_Future_Privacy_EN.pdf.

EDPS (2010), Press Release, Reform of EU Data Protection law: EDPS calls on the European Commission to be ambitious in its approach, 29 April 2010, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2010/EDPS-2010-08_Future_privacy_EN.pdf.

EDPS (2008), *Opinion of the European Data Protection Supervisor on the Final Report by the EUUS High Level Contact Group on information sharing and privacy and personal data protection*, 11 November 2008.

European Parliament and Council (2009), *Regulation (EC) No 444/2009 of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in 48 passports and travel documents issued by Member States*, OJ L 142, Brussels, 6 June 2009, pp. 1-4.

Gutwirth, S., Y. Poulet and P. De Hert, (2010) *Data Protection in a Profiled World*, Springer, Dordrecht

House of Commons, Justice Committee (2010), *Justice Issues in Europe*, Seventh Report of Session 2009-10, Volumes I and II, HC162-1, HC 162-II, London: The Stationery Office, 6 April 2010.

International Civil Aviation Organisation (2009), MRTD Report: Beyond 2020, Montreal.

Lodge, J (2010) 'Quantum Surveillance and 'shared secrets' : a biometric step too far? Brussels, CEPs, June 2010. www.ceps.be

Ploeg I, van der and I. Sprenkels (2010) "Migration and the machine-readable body: identification and biometrics" in: H.Dijstelbloem & A.Meijer (eds.) *Migration and the new technological borders of Europe*, (Palgrave MacMillan, forthcoming).

Snijder, M. (2010), *Het Biometrische Paspoort in Nederland: Crash of Zachte Landing (The Biometric passport in the Netherlands: Crash or Smooth Landing): Verkennde Studie voor het Rapport iOverheid*, WWR (Dutch Scientific Council for Government Policy), the Hague, Webpublication Nr 51.

Sprokkereef, A. and P. De Hert, (2010), "Second Generation Biometrics and Dataprotection", in Mordini, E. & D. Tzovaras, *Second Generation Biometrics* (New York: Springer, forthcoming).