Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

Report on Privacy and Personal Data Protection in the European Union

AEDH – European Association for the Defense of Human Rights
EDRI – European Digital Rights

December 2009

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH,EDRi,AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

1 Introduction and foreword

The entry into force of the Lisbon Treaty brings important developments in the field of privacy and personal data protection. The recognition of personal data protection as a fundamental right, the elimination of the 'pillars' system and the single legal personality conferred to the European Union will lead to major, though not clear yet, modifications.

Moreover, revisions of the legal framework for the fundamental right to protection of personal data in the European Union, in view of addressing the challenges of emerging technologies, new business practices and changing social uses, are likely to bring fundamental changes, which might introduce risks of decreasing the current level of data protection in the Union, while it still needs improvements.

Finally, the adoption of the Stockholm programme, defining the framework for EU police and customs cooperation, rescue services, criminal and civil law cooperation, asylum, migration and visa policy for the period 2010–2014 raises a number of privacy and data protection issues for the future. Coming after the Tempere program of 1999 relying on information exchanges, and then The Hague program of 2004; relying of the "data availability" principles, the Stockholm program is a sorce of main concern in terms of data sharing since it aims at achieving full integration through total interoperability, and full access of databases for police purposes.

It therefore appeared necessary to provide a detailed overview of the current legal and regulatory situation in the Union with regards to privacy and data protection, and to assess this situation with regards to: (i) data protection instruments and institutions; (ii) main issues in terms of legislation, regulation and databases; and (iii) main existing recommendations on emerging technologies. This is the purpose of this report, which by no means claims to be complete. Given the framework of the project, the report takes into account the situation as of August 2009.

It is expected that this report serves as a basis for further updates and analyses, as well as a reference for the assessment of national legislations in member States in the field.

2 Data Protection Instruments and Institutions

Several legislative frameworks concerning data protection apply at the European Union level. Personal data protection in Europe is an important offshoot of the fundamental right to privacy as set out in the Council of Europe European Convention on Human Rights (ECHR) (Art. 8), the International Covenant on Civil and Political Rights (Art. 17) and the EU Charter of Fundamental Rights (CFR) (Art. 8). It has deep roots in post-WWII constitutions and legislation of EU member states, particularly Germany and France - two countries that have contributed heavily to the structure and substance of EC/EU law.

2.1 General Data Protection Legislation under First Pillar

2.1.1 Data Protection in the Internal Market (1995 Data Protection Directive)

First of all, there is 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[1]. This Directive is the primary text on the subject of the protection of personal data at the European level. It develops the 1981 Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[2] with the aim of preventing national laws from prohibiting the free movement of data among Member States by harmonizing national DP Laws in the context of the single market. The legislative base of Directive 95/46 is article 100A of the Maastricht Treaty concerning the freedom of circulation of goods, services and capital.

The Directive applies to the "processing of personal data" (such as collection, recording, storing, dissemination, etc) related to public and private activities covered by the community law, 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. Therefore, the Directive does not apply to the processing of personal data in the area of the Common Foreign and Security Policy, cooperation on justice and home affairs, public safety, and national defense and security (including the economic well-being of the State when the processing operation relates to State security matters). This is important since the article draws a line between the competence of the European Community to enact legislation in connection with harmonization for purposes of constructing a single market, the competence of the European Union to enact legislation in areas of public security, defence, etc., and finally member state criminal law competence. This also explains the proliferation of legislation and regulation at the European level in the field, where different institutions produce their own texts. The Lisbon Treaty might bring changes to this situation, however, with the end of the pillars system, the empowerment of the Parliament, and the integration of the European Charter of Fundamental Rights.

A considerable level of protection is guaranteed through the obligations (e.g. the quality of data, an explicit and legitimate purpose of processing personal data, security and notification to an independent supervisory authority) imposed on those responsible for processing data (public authorities, enterprises, agencies, etc.) and through the rights (to be informed, to rectify incorrect data, to object) conferred on individuals whose data is the subject of processing. For example, data subjects must be informed before personal data relating to him/her are disclosed for the first time to third parties or processed for the purposes of direct marketing and have the right to object, on request and free of charge, to such disclosures or uses. The Directive also prohibits 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. It also includes the provision that personal data should not be sent to any non-member state unless it is established that the recipient state provides a similar level of legal protection to personal data. It establishes purposes and criteria for derogations that Member States may adopt in line with those set up in Convention 108.

---

[1] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

[2] See <http://conventions.coe.int/treaty/fr/Treaties/html/108.htm>

Finally, the Directive establishes in its Article 29, a body named the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, also known as the "Article 29 Working Party" (WP29[3]). The WP29 is composed of representatives of the national Data Protection Authorities. It is and independent body with advisory status, which issues opinions and recommendations.

The European Commission monitors[4] the implementation of the 1995 Directive by Member States, and has started a consultation process[5] in July 2009, "to obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individual's personal data within the EU ".

2.1.2 Protection of Data processed by EU institutions (Regulation (EC) No 45/2001)

The EU institutions and bodies are themselves processing personal data, which protection is equally required. Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[6] was thus enacted to ensure the introduction, the application and the monitoring of the data protection rules in the Community institutions and bodies.

The Regulation covers the general rules on the lawfulness of the processing of personal data in the context of internal telecommunications networks, creates a data protection officer in every Community institution or body and introduces sanctions for breaches.

This Regulation also established an independent monitoring body, the European Data Protection Supervisor (EDPS[7]), which is responsible for the prior checking of processing operations and for giving advice to Community institutions and bodies that are drawing up administrative measures or adopting legislative proposals relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. The statute of the EDPS and its working conditions were established by Decision 1247/2002/EC of the European Parliament, of the Council and of the

---

[3] See <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/>

[4] See <http://ec.europa.eu/justice_home/fsj/privacy/lawreport/>

[5] See <http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm>

[6] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF>

[7] See <http://www.edps.europa.eu/EDPSWEB/>

Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties[8].

Like Directive 95/46, the Regulation applies not only to data movement within the EU but also to personal data sent to third countries or international organisations. Article 9 requires that personal data shall only be transferred to recipients that are not subject to national law adopted pursuant to Directive 95/46 if an adequate level of protection is ensured in the country of the recipient.

2.2 Sectoral Data Protection

In the 1990s, the digitization of telecommunications, as well as the privatization of their market, and the rapid growth of the Internet accentuated the need to protect, taking into account this context, the fundamental right of privacy in general, and the right to the protection of personal data in particular. This has led to the adoption of the Electronic Privacy (E-Privacy) Directive, which complements the general data protection legislation by specifically addressing the telecommunications sector and, after its revision, the electronic communications sector.

2.2.1 E-Privacy Directive 1997

Two years after the adoption of the general Directive of 1995, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector[9] was enacted. It is considered as the first e-privacy Directive since its goal is to protect (natural and legal) persons, and in particular their privacy, in respect of the processing of personal data in the public telecommunications sector (e.g. the integrated services digital networks and the public digital mobile networks).

The Direction provides that Member States should guarantee the confidentiality of communications by providing for adequate national legislation. In particular, the Directive requires that traffic data processed to establish calls must be erased or made anonymous upon termination of the call, except for the purpose of billing during a limited period of time, or for the purpose of marketing of the telecom operator own services, subject to subscriber consent.

Furthermore, the Directive prohibits listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized ànd when it is necessary to safeguard national security, defence, public security, or to prevent, investigate, detect and prosecute criminal offences or unauthorised use of the telecommunications system.

Next to this, the Directive mainly relates to the application of the data protection principles, including security of services and networks; data on communications traffic and billing; the right to receive non-itemised bills; the means to opt in and out the presentation and restriction of calling and connected line identification; guarantees

---

[8] Available at <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_183/l_18320020712en00010002.pdf>

[9] Available at <http://eur-lex.europa.eu/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf>

in case of automatic call-forwarding; personal data contained in directories of subscribers; and unsolicited calls for purposes of direct marketing through any electronic means are only authorised when the subscriber has given prior consent.

2.2.2 E-Privacy Directive 2002

In 2002, 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 (Directive on privacy and electronic communications[10] was passed.

This Directive adapts the previous 1997 Directive to developments in the electronic sector and its market, as part of a broader Telecommunication Package for electronic communications infrastructure and associated services. It thus repeals the 1997 Directive. It regulates the issues concerning the right to privacy and the protection of personal data relating to new commercial practices on the Internet. For example, the choice of an opt-in system for spam-mail, unwanted faxes and automated calling systems. This means that users should give prior permission for receiving unsolicited electronic communications for marketing purposes. As regards 'cookies', users should be provided with clear and comprehensive information on their purposes and should have the right to refuse them through easy means.

However, pursuant to a so called rising concern about state security and in the context of the general war on terror[11], article 15 of Directive 2002/58 allows for limitations of the scope of the protection of personal data afforded in the previous 1997 Directive, in particular the requirement to erase or make anonymous traffic data. Article 15 enables Member States to restrict such rights "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". In essence, article 15 allows states to adopt legislative measures providing for the retention of data for a limited period justified on the grounds specified in this Directive. Notable here is the expansion of state powers from doing what is necessary to pursue terrorists to other unrelated acts including mere 'criminal offences' and unauthorized use of electronic communication systems. Equally notable is the introduction, for the first time ever, of the possibility of blanket and systematic surveillance of personal communications, through the

---

[10] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF>

[11] Right after September 11 attacks, President Georges W. Bush sent a letter on October 2001 to the President of the European Commission, asking to modify the draft 2002 Directive so as to allow for the retention of communications data. See letter at <http://www.statewatch.org/news/2001/nov/06Ausalet.htm>. Despite a harsh petition and letter campaign by an international coalition of NGOs, and despite concerns related to the legal basis of this Directive due to the introduction of Third Pillar provisions in a First Pillar text, the European Council succeeded in providing for data retention possibilities in the 2002 Directive. See account of the whole process by the European Parliament legislative observatory at <http://www.europarl.europa.eu/oeil/file.jsp?id=199162>

retention of traffic data. Thirs first breach, allowed by the 2002 Directive, was later used as the basis of the 2006 Data Retention Directive (see the section dedicated to this Directive in this report).

2.2.3 E-Privacy Directive second revision (2009 Telecom Package)

An amended proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and user's rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sectors and Regulation 2006/2004/EC on consumer protection cooperation[12] is pending. It is part of the Telecoms Package, which is a set of five European Directives currently under modification regulating electronic communication networks.

This legislative proposal covers the changes to the Universal Service Directive and the E-Privacy Directive. The stated aim is to adapt the regulatory framework for electronic communications by strengthening certain consumer and user rights and by ensuring that electronic communications are trustworthy, secure and reliable and provide a high level of protection for individuals' privacy and personal data.

More specifically, the objectives of the present proposals are two-fold: on the one hand, strengthening and improving consumer protection and user rights in the electronic communications sector, by - among other aspects - giving consumers more information about prices and supply conditions, and facilitating access to and use of e-communications, including emergency services, for disabled end-users and on the other hand, enhancing the protection of individuals' privacy and personal data in the electronic communications sector, in particular through strengthened security-related provisions and improved enforcement mechanisms.

In the context of this report, mostly the changes to the E-Privacy Directive are of interest.

The main amendments are introducing mandatory notification of security breaches resulting in user's personal data being lost or compromised (to the subscriber and the national regulatory authority) and information on how to mitigate its possible negative effects; strengthening implementation provisions related to network and information security; strengthening implementation and enforcement provisions to ensure that sufficient measures are available at Member State level to combat spam; ensuring that use of 'spy ware' and other malicious software remains prohibited under EC law, regardless of the method used for its delivery and installation on a user's equipment (distribution through downloads from the Internet or via external data storage media, such as CD-ROMs, USB sticks, flash drives etc.); ensuring that practices such as direct marketing are prohibited unless the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC (inter alia about the purposes of the processing) and is offered the right to refuse such processing by the data controller; clarifying that the Directive also applies to public communications networks supporting data collection and identification devices (including contactless devices such as RFID); and finally, modernising certain

[12] Amending process details available at <http://ec.europa.eu/information_society/policy/ecomm/library/proposals/index_en.htm>

provisions that have become outdated, including the deletion of some obsolete or redundant provisions.

When the text was voted in first reading in the European Parliament in September 2008, serious problems arose on the issues of privacy, network neutrality and regarding the implementation of a mechanism known as "graduated response" (or the "three strikes system") at the European level. For example, despite the stated aim to enhance the protection of individual's privacy, Council's proposals were made to allow the telecommunications industry to collect, store and process traffic data without having to comply with data protection principles and specific obligations that otherwise apply to responsible parties, such as the quality principle or the obligation of fair and lawful processing and to keep the data confidential and secure. Furthermore, because no reference was made to applicable data protection principles that impose time limits for storage of the information or to specific time limits within the article, this Council version would have enabled the collection and processing of traffic data for security purposes for an unspecified period of time.

Next to this, the proposal wanted to introduce a "graduated response" mechanism concerning possible restrictions on end-users' choice of "lawful" content and applications, which would have led to impose technical standards on content filtering and monitoring computing and would have obliged ISP's to monitor the content going through their networks. The so-called Amendment 138, seeking to protect users' rights against the three strikes policy by emphasizing the right to privacy and the right to a fair trial (stating that restrictions to the fundamental rights and freedoms of Internet users can only be put in place after a decision by judicial authorities, save when public security is threatened in which case the ruling may be subsequent), was the subject of an epic battle[13].

Because of the upcoming European parliament elections, further discussions on these delicate issues are postponed until the end of 2009.

2.3 Data Protection under Third Pillar (2008 Data Protection Framework Decision)

These incursions of the Third Pillar into the First Pillar, in addition to the many other measures taken by the European Council in relation to police and judicial cooperation in criminal matters (see section on issues with legislation, regulation and database), one cannot but share the worries[14] of the European Data Protection Supervisor (EDPS), and his suggestions to install within the EU legal system a set of guarantees (e.g. clear and strong provisions on the competence of each national and European supervisory authority and an institutionalised joint role for the respective supervisory authorities) to compensate for the lack of a decent comprehensive legal framework on data protection in the field of cooperation between police and judicial authorities. This was especially needed since the 1995 Directive is not applicable in this sector.

Eventually, the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial

[13] See <http://www.laquadrature.net/en/Telecoms_Package>

[14] Expressed a number of times in his opinions, see <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/OpinionsC>

cooperation in criminal matters[15] was enacted, which has to be transposed before 27 November 2010 by the Member States.

The objective of this Framework Decision (also known as Data Protection Framework Decision or DPFD) is the determination of common rules for the protection of personal data of natural persons processed (e.g. collected, stored, transferred, …) in the framework of police and judicial cooperation in criminal matters at European Union level. The provisions of the DPFD apply to Member States authorities or information systems established on the basis of Title VI of the Treaty of the European Union or the Treaty establishing the European Community, and the competent authorities of the Member States concerning the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system.

The treatment of personal data by Europol, Eurojust, the Schengen Information System and the Customs Information System, as well as those provisions introducing direct access for the authorities of Member States are not affected by this Framework Decision. Also, article 1(4) states that the Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security.

In general, the Framework Decision states that personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data has to be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected, however, further processing is allowed under broad and vaguely defined conditions. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life is also made possible when this is strictly 'necessary' and when the national law provides 'adequate safeguards'. Of course, this is also very vague, which is unacceptable in such a sensitive area, and which constitutes therefore a breach of the principle of legality. Moreover, the provisions apply in this sector only to data that are to be transmitted to other Member States authorities: the DPFD is not applicable to Member State domestic data processed for police and judicial purposes.

Member States must ensure that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies only for certain purposes, only to certain authorities and international bodies, and only if the third State or international body concerned ensures an 'adequate' level of protection, but yet again, broad and vaguely defined exemptions are provided. Member States can even transmit personal data received from or made available by the competent authority of another Member State to private parties if the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law; if there are no legitimate specific interests of the data subject that prevent transmission; and in particular cases transfer is even considered essential for the competent authority. The

[15] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML>

competent authority transmitting the data to a private party can however inform the latter of the purposes for which the data may exclusively be used.

The transmitting authority may, in line with national law and the provisions of the Framework Decision, indicate the time limits for the retention of the data, upon the expiry of which the recipient must erase or block the data or review whether or not they are still needed. This obligation however does not apply if, at the time of the expiry of these time limits, the data are required for a current investigation, prosecution of criminal offences or enforcement of criminal penalties. When the transmitting authority did not indicate a time limit, the time limits according to the provisions of the Framework Decision and the national law concerning the retention of data of the receiving Member State shall apply.

The Framework Decision stipulates that the competent authorities must implement appropriate technical and organisational measures to protect personal data according to the risks represented by the processing and the nature of the data to be protected. Next to this, Member States must provide for effective, proportionate and dissuasive penalties, including administrative or criminal penalties, in case of infringements of the provisions adopted pursuant to this Framework Decision, but alas those are not very strong on the matter of data protection since it resulted in the lowest common denominator. Member States must ensure that data subjects are informed regarding the collection or processing of personal data, the data subject also has the right to expect the controller to fulfil its duties concerning the rectification, erasure or blocking of personal, but yet again exemptions are possible. Member States must also designate one or more independent supervisory authorities to monitor the lawful application within its territory of the provisions adopted by Member States pursuant to this Framework Decision. The fact that supervision is scattered amongst various authorities makes it however less efficient. Also, the proposal of the European Parliament to provide for an independent Working Party on the Protection of Individuals with regard to the Processing of Personal Data with advisory status (in the same way as the Article 29 group provided the 1995 Directive under First Pillar) was not maintained in the final text of the Council. Its proposal to have a reference to the Council of Europe Convention 108 was discarded as well. Another shortcoming of the DPFD, underlined by the EDPS, is that it doesn't deal with the Passenger Name Records (PNR) issue and their transfer to non member States, namely to the USA.

Finally, any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision shall be entitled to receive compensation for the damage suffered. But this will be hard to establish, for example, a decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject is permitted if it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests!

3 Main issues: legislation, regulation and databases

3.1 Legislation and regulation

3.1.1 Crossborder access to Biometric and Genetic Database (Treaty of Prüm)

The Treaty of Prüm was signed on 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, The Kingdom of the Netherlands and the Republic of

Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. The following Council Decisions incorporate the substance of the provisions of the Prüm Treaty into the legal framework of the European Union:

- 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[16].
- Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[17].

The stated goal of the Council Decisions is to step up cross-border cooperation in combating terrorism, cross-border crime and illegal migration by making full use of new technologies, providing for reciprocal access to national databases and allowing for an efficient exchange of information and intelligence between law enforcement authorities of the various Member States (cf. Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union[18]).

In this context, Council Decision 2008/615/JHA contains inter alia provisions on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data (digital fingerprints) and certain national vehicle registration data; the supply of data in connection with major events with a cross-border dimension; the supply of information in order to prevent terrorist offences; and the stepping up of cross-border police cooperation. For the purposes of the supply of data, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

On the one hand, these provisions provide for an interlinking of different national databases on a European level while there are no provisions provided for a supervisory authority on the European level or provisions that lay down a general data protection level (in other words, the above-mentioned DPFD does not apply to this interlinking). As regards the data protection provisions, Council Decision 2008/615/JHA states only that the national law of the various Member States applies, provided that the level of data protection is not lower than the protection laid down in the Council of Europe Convention 108 and its additional Protocol of 8 November

---

16 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF>

17 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF>

18 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2006F0960:20061230:EN:PDF>

2001[19] and that it takes account of Concil of Europe Committee of Ministers Recommendation No R(87)15 of 17 September 1987 to Member States regulating the use of personal data in the police sector[20], also where data are not processed automatically. On the other hand, the provisions of Council Decision 2008/615/JHA provoke certain Member States to create new national databases (e.g. concerning DNA profiles) which they did not have prior to this Council Decision. It has also led some Member States to sign bilateral agreements, on the model of the Prüm-based provisions, with non EU States: the agreement signed by Germany with the USA is one of these examples.

Council Decision 2008/616/JHA lays down administrative and technical provisions as regards in particular the automated exchange of DNA data, dactyloscopic data and vehicle registration data, and other forms of cooperation.

Finally, both Council Decisions state that Member States must take the necessary measures to comply with the provisions of these Council Decisions within one year of this Decision taking effect, with the exception of the provisions concerning "on-line access and follow-up requests" with respect to which the necessary measures shall be taken within three years of this Decision and the Council Decision on the implementation of this Decision taking effect.

3.1.2 Transfer of Passenger Name Records to third countries (EU-US PNR)

Besides some bilateral agreements between Members States and thrid countries, there are agreements at EU level with USA, Canada, and Australia. The related EU legislation in force is:

- Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data[21].
- Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security[22] (2007 PNR Agreement[23])

---

[19] Available at <http://conventions.coe.int/Treaty/EN/Treaties/HTML/181.htm>

[20] Available at <http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf>

[21] Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/canada_ec_230_2006_en.pdf>

[22] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0016:0017:EN:PDF>

- Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service[24]

This report is mainly dealing with the EU-US agreement. The stated goal of this above mentioned agreement is to ensure that passenger name record (PNR) data of persons (that were already being collected by air carriers and airline agencies for commercial purposes and delivery of services, in reservation systems such as the European AMADEUS or the US SABRE systems) on eligible journeys are provided, in 'full respect of fundamental rights and freedoms', to the requesting parties of third countries in order to combat terrorism and organised crime, protect people's 'vital interests' and prevent the flight of individuals from warrants or custody issued against them. In other words, for a very broad and vaguely defined variety of purposes having no relation with the delivery of service. The Council Decision between the EU and the USA is applicable for seven years. It requires airline companies to transfer data to the United States Department of Homeland Security (DHS) concerning passengers transported to or from the United States. Strikingly, this arrangement does not work in both directions for throughout the negotiations it apparently never occurred to the EU to ask for reciprocal surrender of personal data of incoming passengers. The passenger name record (PNR) data are collected from the air carriers, flight tickets and travel documents and concern several categories of personal data: the APIS information (name, civil status, date of birth, nationality, country of residence, etc.); the journey (date of reservation/issue of ticket, travel date, itinerary, baggage, seat number, travel status of passenger, travel agency used); the flight ticket (free tickets, upgrades, ticket issue, price, number, form of payment used and billing); PNR (record locator code, names on PNR, split/divided PNR information and all historical changes made to PNR); all available contact information; OSI (*Other Service Information*), SSI and SSR (*Special Services*) data.

'Sensitive' PNR data (i.e. relating to ethnic origin, philosophical, political or religious beliefs, trade union membership, health and sex life) should be automatically filtered by the DHS. DHS undertakes not to use this information and to delete it promptly unless lives are in danger and the passenger has supplied such information. Under such circumstances, DHS is authorised to use it, provided that it maintains a log of access to these data and deletes them within thirty days. It is required to inform the European Commission (within 48 hours) that it has accessed these data.

DHS receives PNR data 72 hours before the scheduled departure, but may ask to receive them earlier if 'necessary'. If the air carriers have a system complying with DHS technical requirements, they will transmit the data to DHS via a 'push' system otherwise, they will transmit the data via a 'pull' system. However, air carriers have to

---

[23] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:204:0018:0025:EN:PDF>

[24] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:213:0047:0048:EN:PDF>

initiate the transition to a 'push' system. DHS retains the data in an analytical database for 7 years, after which time the data are stored for a further 8 years, but in dormant, non-operational status. They may be accessed only with approval of a senior DHS official. The two parties will reach agreement to determine when PNR data must be destroyed. Only those related to a specific investigation in progress may be retained. DHS may transmit PNR data to the US authorities responsible for law enforcement, public security or counterterrorism and to countries capable of ensuring data protection, but only for the same purposes as those for which DHS received the data, which are vague as previously mentioned. DHS also transmits analytical data flowing from PNR data to the concerned European police and judicial authorities, Europol and Eurojust. The European authorities do the same to the US authorities.

DHS undertakes to guarantee a 'high level of protection' for these data and the Council Decision 'advocates' the application of security measures on data transfers and 'calls on' the parties to respect the fundamental rights and freedoms of passengers, but this is nowhere made explicit. DHS also extends the American Privacy Act provisions to PNR in its possession. Administrative, civil and penal sanctions are therefore provided for in the event of failure to respect privacy and unauthorised disclosure. The EU, US and the aviation industry have promised to cooperate so that passengers are informed about how the governments may use the information concerning them. DHS informs and replies to questions from the public on PNR data through publications in the Federal Register and standard notices made available and published on its website. DHS undertakes not to disclose PNR data to the public, apart from the persons concerned.

This agreement was adopted after several controversies[25] and protests followed the European Commission agreement to the unilateral request from US authorities to airline companies in 2003, that were under the threat to not be allowed to land without sending 72 hours in advance of departure to provide these data.

In 2003, a campaign[26] was organized by the European digital rights organization EDRI and partners, with inter alia complaint letters sent to national data protection authorities by travelers against airline companies having infringed their fundamental rights by disclosing their PNR data to US authorities. Other actions included demonstrations in airports, and participation to press conferences and worksshops organized at in relation with Members of the European Parliament.

The dispute was taken at the EU institutions level when the European Parliament decided in April 2004 to take the European Commission and the European Council to the European Court of Justice (ECJ), on the ground that the EC has exceeded its powers and acted in disrespect of the data protection legislation, by making a highly criticized PNR deal on December 2003 with the US authorities. The European Data Protection Supervisor intervened in the court proceedings in support of the European Parliament. The Article 29 Working Party also published very critical opinion on this deal. The ECJ annulled the 2004 agreement by a decision made on May 2006, judging that it was adopted on a wrong legal basis since the transfer of PNR data to US

[25] The different steps are documented at <http://www.edri.org/issues/privacy/pnr>

[26] See <http://www.edri.org/campaigns/airline/0305> and <http://www.statewatch.org/eu-pnrobservatory.htm>

Authorities constituted processing operations concerning public security and the activities of the State in areas of criminal law, where the Commission has no competence. Two decisions were annulled:

- Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection[27], and
- Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection[28]

Following this annulment by ECJ, a new agreement was negociated. After long and difficult negociations and interim agreements, the final agreement was adopted in July 2007, so-called the 2007 PNR Agreement.

Although the number and categories of data was reduced and better guarantees were provided in comparison to initial and interim agreements, this 2007 agreement still raises criticism[29] as it is not protecting adequately enough citizen rights., while the Data Protection Framework Decision adopted in end 2008 (see above) does not cover the PNR data transfer issue.

3.1.3 EU PNR Travel Surveillance System

While the EU-US PNR agreement was under discussion (see dedicated section), the European Commission came with its own proposal for a EU PNR. It put forward to the European Council on 17 November 2007 a Proposal for a Council Framework Decisions on the use of Passenger Name Record (PNR) for law enforcement purposes[30]. The plan is almost similar to the EU-USA PNR agreement. The EU PNR plan was part of a new package of proposals "aimed at improving the EU's capabilities in the fight against terrorism."

The stated goal of the proposed EU-PNR system is to oblige air carriers to make the PNR data of passengers of international flights available to the competent authorities of the Member States for the purpose of analysing the terrorist and criminal threat and to use in the context of individual inquiries before the passengers board the aircraft.

Currently air carriers have an obligation to communicate on request Advance Passenger Information (API) data to the competent authorities of the Member States

---

[27] Available at <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00830083.pdf>

[28] Available at <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf>

[29] Most notably from the EDPS and the European Fundamental Rights Agency.

[30] Available at <http://www.statewatch.org/news/2008/apr/eu-pnr-7656-rev2-08.pdf>

to enhance border control and to fight illegal immigration under Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data[31]. The information contained in the API data (which are basically biographical data and are recorded in the 'machine readable zone' of EU passports and are normally collected at flight check-in) can also help to identify known terrorists and criminals by running their names against alert systems such as the SIS, but according to the Council does not provide an answer for 'unknown' terrorists. That is why the Council proposes a EU PNR-system, since it would provide for a tool to carry out risk assessments of persons for obtaining intelligence and for making associations between known and unknown people. However, Council Directive 2004/82/EC was hardly transposed by Member States, so it is difficult to maintain that it didn't suffice.

The proposal for an EU PNR-system concerns passengers on international flights serving the territory of a Member State, but also looks into the possibility to include passengers for intra-Community flights and to move beyond air traffic (e.g. transport by sea, rail etc.), but this depends on the financial and practical implications involved. In other words, although the PNR system is a very invasive tool for privacy, ethical and societal implications are not considered. Even more, similar data are already being, and will continue to be, collected by some Member States at national discretion (France, Denmark and most notably the UK with its E-Border system).

The proposal provides for the collection of 19 categories of personal data gathered by air carriers on air passengers coming into and leaving the EU space, including phone number, e-mail address, travel agent, full itinerary, billing data and baggage information,are more or less identical to those being collected under the controversial agreements between the EU and the USA. Sensitive data should be deleted immediately.

A Passenger Information Unit will be responsible for collecting the PNR data from the air carriers or the intermediaries and for analyzing them in respect of possible risk profiles according to criteria and guarantees provided for under national law. The Passenger Information Unit of a Member State shall transmit the PNR data of individuals identified for further examination to the relevant competent authorities of the same Member State, e.g. those responsible for the prevention or combating of terrorist offences and organised crime. No enforcement action can be taken by the Passenger Information Units and the competent authorities of the Member States only by reason of the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation. However, this can result in an interrogation or a refusal to enter the territory.

Air carriers shall make available the PNR data to the Passenger Information Unit 24 hours before the scheduled flight departure and immediately after flight closure, but the Passenger Information Unit may ask those data prior to the 24 hours when there is an indication that early access is 'necessary' to assist in responding to a specific threat related to terrorist offences and organised crime. Air carriers whose databases are established in a Member State of the European Union must transmit (preferably by electronic means) the PNR data to the Passenger Information Units or the designated intermediaries using the "push method". Air carriers whose databases are established

---

[31] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:261:0024:0027:EN:PDF>

in third countries shall also be required to use the "push method" if technically possible, if not they can use a “pull method”. The proposal speaks of a time limit, after which all transmissions of PNR data shall be made electronically, using secure methods (by using common protocols and encryption standards) to ensure the security of the data during transmission and their readability by all parties involved.

The data will be stored in an active database for five years during which Passenger Information Units or competent authorities of the Member States shall have the right to access them for the prevention or combat of terrorist offences and organised crime. After five years, the PNR data shall be stored for another eight years in a ‘dormant’ database (also in accordance with the EU-USA agreements). During this period, the PNR data may be accessed, processed and used only with the approval of the competent authority and only in exceptional circumstances in response to a specific and actual threat or risk related to the prevention or combat of terrorist offences and organised crime. Access to such data shall be ‘limited’ to personnel of the competent authorities which will be specifically authorised for this purpose. Member States shall ensure that the PNR data are deleted from the databases of their Passenger Information Unit upon the expiry of the period of eight years, but the Passenger Information Units are allowed to retain the PNR data for longer periods in cases where the data is being used for an ongoing criminal investigation of a terrorist offence or an organised crime against or involving the data subject. Such data shall be deleted from all records and files once such an investigation is concluded. Next to this, PNR data may also be transmitted to law enforcement authorities of third countries (in compliance with (inter)national law) if the law enforcement authorities of the third country shall only use the data for the purpose of preventing and fighting terrorist offences and organised crime, and such third country shall not transfer the data to another third country without the express consent of the Member State.

Member States shall ensure that air carriers inform passengers of international flights about the provision of PNR data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use, and about the possibility of exchanging and sharing of such data. Member States shall ensure, in conformity with their national law, that dissuasive, effective and proportionate sanctions, including financial penalties, are provided for against air carriers and intermediaries which do not transmit data or transmit incomplete or erroneous data or otherwise infringe the national provisions adopted pursuant to this (proposal for a) Framework Decision. In case of repeated serious infringements, these sanctions shall include measures such as the immobilisation, seizure and confiscation of the means of transport, or the temporary suspension or withdrawal of the operating license. Also, Member States must ensure that the 2008 Data Protection Framework Decision is applicable to the processing of personal data under this proposal for a Framework Decision. However, since this Framework Decision does not provide for an efficient and high level data protection regime, there are no real sanctions provided for unauthorised use of PNR data by the Passenger Information Units or the ‘competent’ authorities.

The draft Framework Decision received severe criticism, either for lack of respect of fundamental rights or for not going further enough, depending on the origin of the reactions.

The joint opinion of the Article 29 Working Group on Data Protection and the Working Party on Police and Justice of December 2007[32], the European Data Protection Surpervior opinion of 20 December 2007[33], the European Fundamental Rights Agency opinion of 28 October 2008[34] and the European Parliament Resolution of 28 November 2008[35] have all expressed strong reservations on the need and the added value that a EU-PNR scheme would bring, as well as on the proportionality and impreciseness of many provisions.

On the other hand, some Member States, with the UK in the lead, expressed strong disagreement on the 2007 EU-PNR proposal, since they wanted to go further in this matter. The demand was to extend the PNR scheme to all types of travel (air, land and sea), not only in and out the EU borders, but also between EU countries and even within each country. They also wanted the data and information gathered to be used not just for entry-exit, but also for any law enforcement purpose.

The Council thus started discussions towards a revision of the draft Framework Decision in 2008[36].

3.1.4 European biometric passports

The concerned legislation is Council Regulation 2252/2004/EC of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States[37], and Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States[38]. It is complemented by technical specifications on the standards for security features and biometrics in passports and

---

[32] Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf>

[33] Available at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf>

[34] Available at <http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf>

[35] Available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0561+0+DOC+XML+V0//EN>

[36] See accounts of these discussions and some Council internal documents at <http://www.statewatch.org/eu-pnrobservatory.htm>

[37] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0001:0006:EN:PDF>

[38] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:0004:EN:PDF>

travel documents issued by Member States established in Commission Decisions[39]

The stated purpose of this Regulation is to lay down harmonised standards for security features and biometrics in passports and travel documents issued by the Member States to protect against falsification and to establish a reliable link between the genuine holder and the document. However, under the current EC Treaty, the Council had no competence to harmonise provisions on passports, according to Article 18 EC. The fact that Regulation 2252/2004 was enacted without co-decision of the European Parliament and the possibility to modify the Regulation provisions by comitology procedure, and thus without democratic oversight, made it all the more problematic.

The Regulation stipulates that passports and travel documents have to include a storage medium, which shall contain a facial image and two fingerprints (of the left and right index finger) in interoperable format, thus going even beyond international regulation from the International Civil Aviation Organization, which requires only the facial image. The 2004 Regulation concerns every EU citizen, but stipulates no age limit for giving fingerprints. The amending Regulation of 2009 introduces a provisional age limit following technical considerations, not ethical ones. Children under the age of 12 (rather than 6), next to people who are physically unable to give fingerprints, will be exempt from the requirement to give fingerprints. The 2009 Regulation also incorporates the principle of "one person-one passport" as a supplementary security measure, in particular in order to provide additional 'protection' for children. Moreover, the above-mentioned data are the minimum safety requirements; individual Member States can add features.

These sensitive data shall be collected and stored in the storage medium of passports and travel documents, with a view to delivering such documents and to verify the authenticity of the document and the identity of the holder at border check points. Member States will thus dispose of the fingerprints of every European citizen, whether they are criminal suspects or not. The Regulation does not provide a legal basis for storage of the data in a national database, leaving decision on this matter to national law. It does not specify either which authorities and bodies are authorized to have access to the data contained in the storage medium of the documents, or in national databases when they exits,also referring this to national legislation. This is very problematic as some Member States have indeed set up such a national centralised database: this is the case in France, for instance, where the implementes regulation is currently under legal complaint filed by two French NGOs[40].

Another problem is that additional technical specifications (such as additional security features and requirements, technical specifications for the storage medium of the biometric features and their security, requirements for quality and common standards for the facial image and the fingerprints) can be, and have already been, introduced in accordance with the relevant comitology procedure and thus without democratical oversight. However, it is clear that the storage medium on the passports and travel documents will consist of an RFID-chip.

---

[39] See <http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm>

[40] See <http://www.iris.sgdg.org/info-debat/comm-passeport0708.html>

Radio-frequency identification (RFID) is the use of an object (typically referred to as an RFID tag or chip) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions. The second is an antenna for receiving and transmitting the signal. There are generally two types of RFID tags: active RFID tags, which contain a battery and can transmit signals autonomously, and passive RFID tags, which have no battery and require an external source to provoke signal transmission. The electronic chip required by the ICAO, and agreed on by comitology procedure, must conform to ISO/IEC 14443 A/B, which means that it is an active RFID tag, but with a maximum reading range of less than 10 cm.

In an effort to make passports more secure, several countries have implemented RFID-chips in passports, but the encryption measures can easily be countered, which has been proven already by many researchers in various Member States that use already RFID passports, such as Belgium. For example, researchers have been able to clone passport data while the passport is being mailed to its owner. Where a criminal used to need to secretly open and then reseal the envelope, it can now be done without detection, adding some degree of insecurity to the passport system. Next to this, it becomes possible to gather sensitive data about an individual without consent since the tag can be read at a distance without the knowledge of the individual. Using a simple commercial reader, one can read all the electronic information stored in the passport. Still worse, this technology provides a way to know the presence of a passport's bearer at some place and at a specific time, thus raising the traceably problem. Consequently, the ICAO has specified amongst others many requirements and recommendations to countermeasure these issues, in particular a Basic Access Control and Secure Messaging mechanism but even these aren't infallible.

Member States have to apply Council Regulation 2252/2004 at the latest by 28 December 2007, as regards the facial image, and by 28 June 2009, as regards fingerprints. Many Member States probably won't be ready for this second deadline.

The European Biometric passport has been facing harsh criticisms, not only from NGOs but also from the Article 29 group and the EDPS, as well as from the European Parliament, and protest campaigns since its initial discussions steps in 2003. This opposition is also related to national level measures and plans by Member States, not only regarding the national implementation of the biometric passport, but also in relation to the introduction of national biometric identity cards[41].

3.1.5 Communication data retention

On data retention, after the first breach opened with Article 15(1) of the 2002 E-Privacy Directive, communication data retention became mandatory with Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly

[41] See regular reporting on these developments at <http://www.edri.org/issues/technology/biometrics>

available electronic communications services or of public communications networks and amending Directive 2002/58/EC[42].

The stated goal of the Data Retention Directive is to harmonise Member States provisions concerning the obligations of providers of publicly available electronic communications services (only those that are normally provided for remuneration and therefore not free services) with respect to the retention of certain data in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

The Directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It applies to data necessary to trace and identify the source and to identify the destination of an electronic communication, through fixed or mobile telephony (calls and text messages) or through the Internet (access, email and IP telephony). It does not apply to the content of electronic communications, including information consulted using an electronic communications network. Nevertheless, the systematic examination of traffic and location data produces more or less a complete overview of certain aspects of people's lives (e.g. their circle of acquaintances and their movements). Next to this, traffic and location data can be analyzed automatically, in connection with other data, in search for specific patterns according to certain criteria (i.e. data mining). Thus, retaining traffic and location data creates opportunities that are not possible by processing the content of communications and deserves as a consequence an appropriate level of protection.

Member States must ensure that the categories of data specified are retained for periods of not less than six months and not more than two years from the date of the communication. Nevertheless, a Member State facing 'particular circumstances' that warrant an extension for a limited period of the maximum retention period may take the necessary measures.

The Directive stipulates that providers of publicly available electronic communications services or of a public communications network should respect as a minimum certain prescribed data security principles. Next to this, Member States must provide for effective, proportionate and dissuasive penalties, including administrative or criminal penalties, in case of any unauthorized access to, or transfer of, the to be retained data. Finally, Member States must also designate one or more independent supervisory authorities to monitor the lawful application within its territory of the data retention provisions. The fact that supervision is scattered amongst various authorities makes it however less efficient.

Even though the stated aim of the Directive is harmonisation, the Directive leaves several open questions and room for implementation choices by Member States concerning the data to be retained data (e.g. extension to web activity logs, banking data, etc), the retention period, the terms of access to the retained data (e.g. for the purpose of prevention -although the European Parliament explicitly prohibited this possibility- of crime in general) and the chosen handover interface of the retained data between the providers and the law enforcement authorities (LEAs) (e.g. a manual

[42] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

handover interface, a completely automated electronic handover interface, a centralized storage by the LEAs, and the outsourcing of data retention to private companies).

The Data Retention Directive was adopted very quickly without adequately reflecting on the necessity and proportionality of the measure, e.g. by outweighing the framework against other solutions (such as legal interception) and by reflecting on the overall consequences for society. Data retention is an invasive tool that interferes with the right to privacy and which turns all 450 million European citizens into potential suspects. Data retention is a far cry from the recognition, a mere 15 years ago, that entities, including states, collecting too much data have tended to abuse the data at the expense of individuals and fundamental rights. Moreover, there are many technological ways to circumvent the retention measures and it can be estimated that organised crime will know these techniques very well, making it virtually impossible for law enforcement authorities to actually trace them down, and thus rendering a generalised data retention useless to fight organised crime.

The Data Retention Directive had to be implemented in the European Member States at the latest by 15 September 2007. Concerning the Internet communication data, the deadline was 15 March 2009. Various member states are late in implementing this Directive. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the various applications of this Directive and consider whether amendments with regard to the list of the to be retained data and the retention period in the Directive are advisable.

The Data Retention Directive is the result of a long story that need to be read in the light of competition between EU institutions. Soon after the 2002 E-Privacy Directive adoption in May, the Council circulated in November 2002 a questionnaire to membser states on their needs with regards to data retention[43]. Then in April 2004, France, Ireland, Sweden and the UK proposed a Council Data Retention Framework decision[44]. It included mandatory retention of communication data, during 12 to 36 months. As the Framework Decision proposal, it clearly appeared that data retention, putting an obligation on ISPs and telecom operators was a First pillar matter, not a Third Pillar one, and the Framework Decision project had to be abandoned, and replaced by the Directive proposal by the European Commission

Data Retention plans have faced severe opposition[45], during their proposal as a Framework Decision and later on during Data Retention Directive discussion as well as after its adoption, and now also at national level in the course of its implementation. The opposition came from other European Institutions (most notably Article 29 Group[46] and the European Parliament[47], from the industry and, through

[43] See <http://www.effi.org/sananvapaus/eu-2002-11-20.html>

[44] Available at <http://
register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf>

[45] Documented at <http://www.edri.org/issues/privacy/dataretention>

[46] See
<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf> and

several protest actions and campaigns, from NGOs and civil society as a whole. According to theopposition source, several arguments have been raised, from wrong legal basis to the violation of human rights as well as the involved burden cost.

Ireland, later on joined by Slovakia, challenged the Data Retention Directive before the European Court of Justice (case C 301/06) on the grounds that Directive 2006/24/EC was founded on the wrong legal basis. As 'friends of the Court', 43 NGOs expressed their support of the legal action in April 2008, but arguing that the Directive is first and foremost illegal on human rights grounds. However, on 10 February 2009 the Grand Chamber of the Court decided that the Directive was founded on the right legal grounds, but gave no verdict on the most relevant question whether or not the Directive was in violation of human rights.

Successive campaigns have been run by NGOs against the Data Retention Directive. In September 2004, a statement against data retention plans jointly written by Privacy International and EDRI was signed by 90 NGOs and 89 private companies[48], arguing that such data retention is necessarily a hazardously invasive act and identifying data retention plans as "invasive, illusory, illegal, and illegitimate". In July 2005, a petition campaign was launched by EDRI, with the same arguments. The petition was closed on November 2005 with 58.000 signatures[49]. On September 2006, a German national coalition started a campaign against data retention[50], which raised growing interest nationally and led to important massive actions, both through street demonstrations and through class action law suit challenging the national implementation of the Data Retention Directive. Other national complaints by NGOs are pending in Ireland, and other countries as well.

3.2 Databases and agencies

3.2.1 Schengen Information System

The Schengen Information System (SIS) is founded on the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

It was supplemented on 19 June 1990 by the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the

---

<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf>

[47] See <http://www.europarl.europa.eu/oeil/file.jsp?id=5275032>

[48] Available at <http://www.edri.org/campaigns/dataretention/0409>

[49] Available at <http://www.dataretentionisnosolution.com/>

[50] See <http://www.vorratsdatenspeicherung.de/component/option,com_frontpage/Itemid,1/lang,en/>

gradual abolition of checks at their common borders[51]. Finally, with the signing on 2 October 1997 of the Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and related Acts[52], the Schengen Agreements were incorporated into European Community law. All these measures, together with the corresponding decisions, declarations, protocols and accession agreements that followed, constitute the Schengen acquis. In order to adapt the Schengen acquis, all signatory States must accept modifications in full.

The legislative framework has since been amended by:

- Council Decision 1999/307/EC of 1 May 1999 laying down the detailed arrangements for the integration of the Schengen Secretariat into the General Secretariat of the Council[53].
- Council Decision 2001/886/JHA of 6 December 2001 on the development of the second generation Schengen Information System (SIS II)[54]
- Council Regulation 2424/2001/EC of 6 December 2001 on the development of the second generation Schengen Information System (SIS II)[55].
- Council Regulation 871/2004/EC of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism[56].
- Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism[57].

---

[51] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:EN:PDF>

[52] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:11997D/AFI/CE:EN:HTML>

[53] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:119:0049:0052:EN:PDF>

[54] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:328:0001:0003:EN:PDF>

[55] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:328:0004:0006:EN:PDF>

[56] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:162:0029:0031:EN:PDF>

[57] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:068:0044:0048:EN:PDF>

- Regulation 1160/2005/EC of the European Parliament and of the Council of 6 July 2005 amending the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders, as regards access to the Schengen Information System by the services in the Member States responsible for issuing registration certificates for vehicles[58].
- Regulation 1986/2006/EC of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates[59].
- Regulation 1987/2006/EC of the European Parliament and of the Council of 20 December 2006 on the establishment, operation, and use of the second generation Schengen Information System (SIS II)[60].
- Council Regulation 1988/2006/EC of 21 December 2006 amending Regulation 2424/2001/EC on the development of the second generation Schengen Information System (SIS II)[61].
- Council Decision 2006/1007/JHA of 21 December 2006 amending Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II)[62].
- Council Decision 2007/471/EC of 12 June 2007 on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Czech Republic, the Republic of Estonia, the Republic of Latvia, the Republic of Lithuania, the Republic of Hungary, the Republic of Malta, the Republic of Poland, the Republic of Slovenia and the Slovak Republic[63].

---

[58] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:191:0018:0021:EN:PDF>

[59] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0001:0003:EN:PDF>

[60] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0023:EN:PDF>

[61] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:411:0001:0005:EN:PDF>

[62] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:411:0078:0081:EN:PDF>

[63] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:179:0046:0049:EN:PDF>

- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)[64]
- .Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)[65].
- Council Regulation 1104/2008/EC of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)[66]
- Parliament and Council Regulation 265/2010 of 25 March 2010 amending the Convention Implementing the Schengen Agreement and Regulation (EC) No 562/2006 as regards movement of persons with a long-stay visa[67]

Other documents concerning the migration from SIS I to SIS II and the establishment of an agency for the system operational management are in development[68].

The stated goal of SIS is to compensate for the abolishment of systematic controls at the internal borders of the Schengen area, i.e. the territory of the signatory States, by creating a common information system that allows the competent authorities in the signatory States to obtain information and sent out alerts regarding certain categories of persons and goods and thus maintaining order and public security while 'respecting the free movement of persons'. Although not explicitly mentioned, SIS is also used as an instrument for immigration control. However, with the migration to SIS II, new functions are introduced, and SIS would become not only a reporting system but an investigation system as well.

The SIS database is operational since 26 March 1995, when the Convention implementing the Schengen Agreement entered into force. The Schengen area gradually extended and currently consists of twenty-five European countries, together with Norway and Iceland. The Member States that joined the EU on 1 May 2004 are bound by the entire Schengen acquis, but certain provisions will apply to them only

---

[64] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:205:0063:0084:EN:PDF>

[65] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:299:0043:0049:EN:PDF>

[66] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:299:0001:0008:EN:PDF>

[67] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:085:0001:0004:EN:PDF>

[68] See texts relating to Schengen information system (SIS II) at <http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm>

after border controls have been abolished and SIS II becomes operational. Ireland and the United Kingdom opted out of Schengen's border control arrangements, but participate in certain provisions relating to judicial and police cooperation, among which the SIS database. Denmark signed the Schengen Agreement, but it can choose whether or not it applies new measures. Associated countries, such as Iceland, Norway and Switzerland, participate in discussions on the development of the Schengen acquis but have no right to vote. SIS II is not yet operational and a recent press release of a JHA Council meeting confirms that the date for migration from SIS I+ to SIS II, set for September 2009, is no longer realistic.

The SIS database contains only basic information and works on a 'hit/no hit basis'. At present, the SIS contains six kinds of alert, notably people wanted for arrest and extradition, people to be refused entry to the Schengen area (the biggest group), missing and dangerous persons, people wanted to appear in court, people to be placed under 'discreet surveillance' or wanted for 'specific checks' and finally, lost and stolen objects. There are serious concerns about the broad grounds under which people can be registered as 'illegal aliens to be refused entry', or those for 'discreet surveillance' and 'specific checks'. On top of this, interpretation of these categories is not unanimous amongst the various signatory States. After all, one of the principal problems of transnational information exchange between law enforcement authorities is the simple fact that the countries exchanging information exhibit strong cultural and legal differences between them. Nevertheless, in principle, every signatory State is expected to act upon the alerts of other signatory States, despite a difference in interpretation. As a result, all the signatory States have to enforce a policy of exclusion pursued by the more zealous among them. The competent authorities of the signatory States foster the SIS-database and information is stored according to the legislation of each country. The retained information concerning persons are the name and surname, initial of second forename, date and place of birth, distinguishing features, sex, nationality and four categories of information for police officers (whether the person is armed or violent, the reason for the report, and the action to be taken). At present, supplementary information can be exchanged in standard forms through the Sirene Bureaux, a dedicated communications system designed for this purpose, after a hit on the SIS.

However, SIS II is to change all this. SIS II, which is still in preparation, will integrate the new EU Member States and will provide for five critical new functions. First, there is the addition of new categories of alert, such as children to be prevented from leaving the Schengen area, 'violent troublemakers' (a very broad and vague category), suspected terrorists, and visa-overstayers (by linking it to VIS). Secondly, there is the addition of new categories of data, including 'biometric' data (such as digitised photographs, fingerprints, and in the future perhaps DNA) and, if applicable, the information on the form of European Arrest Warrants. Thirdly, there is the interlinking of alerts. The interlinking of SIS alerts, which is currently not possible, may appear uncontroversial and even logical. However, the result is that supposition and 'intelligence' will creep steadily into SIS II. This is another significant extension of the 'investigative' powers of the SIS and, needless to say, greatly improves the chances of innocent people suffering serious repercussions as a result of being 'associated' with criminals (or even suspected criminals) and/or specific crimes or criminal phenomenon's. Fourthly, there is a widened access to the SIS (including access for the security and intelligence services), and finally, a shared technical platform with the Visa Information System (VIS) and Eurodac. The broad law

enforcement access to VIS and Eurodac provides, in conjunction with SIS II, an EU-wide fingerprint database of wanted persons, suspects and all visa entrants and asylum applicants. This will fundamentally transform the role of the SIS. At present the system is used to verify that individuals entering an EU Member State, or caught up in that state's criminal justice system, are not banned or wanted by another member state. The new functionalities will allow SIS II to be used as an investigative tool, enabling speculative searches in which people registered on the SIS will form a key suspect population.

The current retention period of the above-mentioned alerts in the SIS is limited to three years, which can be renewed if necessary. In a number of Schengen States the three-year retention period is routinely renewed, which has resulted in a de facto increase in the standard period of retention for many alerts. SIS II however, wants to extend this retention period to five years concerning alerts on 'illegal aliens to be refused entry' and to ten years concerning alerts on persons wanted for arrest and surrender or extradition, as well as persons wanted in order to ensure protection or prevent threats, and persons wanted for judicial procedure. Next to this, there are no provisions for an annual review of the need for continued retention. The competence to modify, complete, rectify, update or erase the information in SIS is reserved to the competent authority of the signatory State that inserted the particular information into SIS.

Access to SIS previously was 'restricted' to police officers, border guards, immigration officers and customs officials who could only check the data -through means of an automated search procedure- relevant to the exercise of their duties. However, the number of authorised users has already been enlarged in preparation of SIS II, including the state security and intelligence services, public prosecutors and judges, ministerial departments, vehicle registration authorities, Europol and Eurojust. Thus, not only will the ten new EU Member States plus the UK and Ireland participate in SIS II, but several new user groups will have access. The negative relationship between data security and the number of people that have access to that data should be cause for concern. Also, the design of SIS II is such that it will be possible to add new users at a stroke, including the possibility to give partial access with a purpose different from the original one set out in the alerts. This is a flagrant breach of one of the fundamental principles of data protection -that data may only be used for the purpose for which it was collected- and also clearly prohibited in the Schengen Convention.

Concerning the transfer of personal data to third parties or international organisations (e.g. Interpol), this is prohibited except if explicitly provided for in EU law, for example in the framework of an EU agreement, and if an 'adequate' level of protection is guaranteed. However, this has a wider implication in view of the proposals to connect SIS II to VIS and Eurodac. Also, it is not clear which bodies will possess the power to make decisions regarding the transfer of data and on what criteria, nor whether access will be granted to private organizations as well as public bodies.

The architecture of SIS (current version is SIS I+) consists of an interconnection of national databases (N–SIS), via a secured communication network, with a central server in Strasbourg (C–SIS) sending and receiving data to and from the national databases (radial shape). Information is supplied by each contracting State via its N–SIS and distributed subsequently via C–SIS among all other N–SIS. Therefore, the

content of all N–SIS is identical, and it is identical with the content of C–SIS (parallel storage). The search for information in each signatory State only takes place in the N–SIS of this State. The databases only contain the indispensable information (the so–called ‘alert data’) allowing the identification of a person or an object and the necessary action to be taken. The SIS is supplemented by the national SIRENE Bureaux (Supplementary Information Request at the National Entry) which provides additional information through a protected telecommunication system (SISNET). The system architecture of SIS II will basically be the same as the old, still operational SIS, but new functions will be added (e.g. more categories of alert and of data, the interlinking of alerts) and its technical platform will be shared with VIS and Eurodac. The number of authorised users has already been enlarged in preparation of SIS II. Pending SIS II becoming operational, the JHA Council of December 2006 gave its endorsement to the SISone4all project. SISone4all is a temporary solution designed to connect nine EU-2004 Member countries to the existing version of SIS1+.

There are also discussions about the future management of SIS II and hence the possibility of entrusting the central component to a separate agency that will be responsible for certain tasks (e.g. help desk, data protection). Next to this, there are discussions about externalising certain activities, such as the delegation of executive responsibilities to national public bodies and agencies, and even the outsourcing of responsibilities to private sector firms.

In conformity with basic data protection principles, specific rights are recognised by the Schengen Convention for both nationals and non-nationals of Member States in the Schengen area. These are basically the right of access (direct or indirect) to data relating to them stored in the SIS, the right to rectification when data are factually inaccurate or unlawfully stored, and the right to bring before the courts or competent authorities an action to correct or delete incorrect data or to obtain compensation. The request for review may be refused if this should prove necessary due to the execution of a measure, protection of rights and liberties of third parties and always when a clandestine recording is in place. The request to review personal data pertaining to you, and the request to correct or delete the incorrect illegal personal data pertaining to you, may be submitted by any individual at the competent body of any country within the territory of the signatory states. The procedure to institute the request for review, correction or deletion shall be governed by the legislation of the country where the request was lodged.

Signatory states have the obligation to ensure the correctness, the up to datedness and the legality of the integrated data, and to use these data only for the finality stated by the relevant articles of the convention. If one of the contracting parties which has not issued the alert has evidence suggesting that an item of data is factually incorrect or has been unlawfully stored, it advises the contracting party issuing the alert. The issuing country is obliged to check the communication and, if necessary, correct or delete the item in question. If the contracting parties are unable to reach agreement, the contracting party which did not issue the alert shall submit the case to the Joint Supervisory Authority (JSA).

The Schengen Convention provides for a system of data protection supervision which distinguishes between the national data protection authorities (DPAs) who supervise the national part of SIS (i.e. N-CIS and SISNET) and a common, but independent,

control authority, the Joint Supervisory Authority[69] (composed of representatives from the national DPAs), to supervise the central system of SIS (i.e. C-SIS). The tasks of the JSA are supervising the technical support function of the SIS and checking that the provisions of the Schengen Convention are properly implemented; examining any difficulties of application or interpretation that might arise during the operation of the SIS; studying any problems that may occur with the exercise of independent supervision by national supervisory authorities; studying any problems that may occur in the exercise of the right of access to the system; and drawing up harmonized proposals for joint solutions to existing problems. The supervision of the technical architecture of the SIS II will be monitored by the EDPS concerning the data processing activities of the Commission. However, clear provisions on the competence of each supervisory authority and an institutionalised joint role for the respective supervisory authorities are lacking. Nevertheless, this is particularly important as not all states that apply the Schengen acquis are members of the EU. There should be appropriate supervision at both national and EU level.

3.2.2 Visum Information System

The legislative framework of the Visa Information System (VIS) is founded on Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)[70].

The Decision has since been amended by:

- Regulation 562/2006/EC of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code)[71].
- Commission Decision No 2006/752 of 3 November 2006 establishing the sites for the Visa Information System during the development phase[72].
- Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences[73].

---

[69] See its website at <http://www.schengen-jsa.dataprotection.org>

[70] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:213:0005:0007:EN:PDF>

[71] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0001:0032:EN:PDF>

[72] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:305:0013:0014:EN:PDF>

[73] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0129:0136:EN:PDF>

- Regulation 767/2008/EC of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)[74].Regulation 81/2009/EC of the European Parliament and of the Council of 14 January 2009 amending Regulation 562/2006/EC as regards the use of the Visa Information System (VIS) under the Schengen Borders Code[75].
- Regulation 390/2009/EC of the European Parliament and of the Council of 23 April 2009 amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications[76].

The personal data of every person applying for a visa that are retained in the VIS database are the alphanumeric data on the applicant and on the visas requested, issued, refused, annulled, revoked or extended; digitised photographs; and in the future biometric data. Using biometrics in information systems however is never an insignificant choice, especially when the system in question concerns such a huge number of individuals. Biometrics change irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine readable' and subject to further use. According to the EDPS, this sensitive nature of biometric data requires that the introduction of obligations to use these data should only take place after a thorough assessment of its risks and should follow a procedure allowing full democratic control. Next to this, the recent decision (Regulation No 767/2008) to include short-stay visas in the VIS will lead to a massive collection and processing of personal and biometric data concerning a huge number of persons.

Each application file will be stored in the VIS for five years. Only the duly authorised staff of the concerned visa authority will have the right to enter, amend or delete data to the VIS. Outsourcing the processing of visa applications to a private company should be admissible only if it involves a place under diplomatic protection, and is based on contractual clauses providing for effective oversight and liability of the contractor, otherwise it would create huge security problems concerning the protection of the personal and biometrical data.

The competent authorities responsible for visas, those responsible for checks at the external borders, for immigration and asylum, for internal security and finally Europol have access to certain categories of VIS data under specific conditions and to the extent that the data is required for the performance of their tasks.

---

[74] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0060:0081:EN:PDF>

[75] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:035:0056:0058:EN:PDF>

[76] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:131:0001:0010:EN:PDF>

The VIS was originally established as a border management system by preventing the bypassing of the criteria established by the Dublin II Regulation, by facilitating the fight against documentary fraud, by facilitating checks at external border checkpoints, and by assisting in the return of illegal immigrants.

This however, changed with Council Decision 2008/633/JHA. Since then, the VIS will also be used as an instrument to combat terrorism and crime. Despite the fact that most of the visitors to the EU are legitimate travellers who do not have any connection with criminality whatsoever (nor do illegal immigrants or unauthorised entrants) they are considered as a potential threat to the internal security of the Member States. Consequently, the migration to VIS II creates a tendency to retain more and more sensible personal data (e.g. biometrics), to enhance interoperability between European databases (e.g. Eurodac, SIS II, …), to extend access to the VIS database to Europol and national authorities responsible for internal security and to allow processing of the data for other purposes. Data protection rules require nevertheless that in principle personal data are only processed for reasons compatible with the reason(s) for which they were originally collected. Moreover, many of the sensitive issues concerning VIS are decided upon exclusively by means of a comitology procedure (which is largely hidden from public view and debate), but in the light of their impact on fundamental rights including the protection of personal data, these should be the subject of primary legislation.

The Visa Information System (VIS) is based on a centralised architecture and consists of a central information system, the "Central Visa Information System" (CS-VIS), and an interface in each Member State, the "National Interface" (NI-VIS), which provides the connection to the relevant central national authority of the respective Member State, and the communication infrastructure between the Central Visa Information System and the National Interfaces. Also, in the second generation of VIS, individual passports will have an electronic chip carrying the personal data of the applicant, including its biometric data. The EDPS criticizes the decision to retain biometric data in a central database for years if the same information is already on an electronic chip on the visa, all the more with the recent Council Decision 2008/633/JHA that allows a broad access to the VIS database by law enforcement, security and information services.

The legislative framework provides also for certain limited safeguards. For example, every person has the right to obtain communication of the data relating to him/her recorded in the VIS and of the Member State that transmitted it to the VIS and to request that inaccurate or unlawfully recorded data be deleted. To guarantee this right any person can bring an action or a complaint before the competent courts of that Member State if necessary. When it is proven that a person, or Member State, has suffered damage as a result of an unlawful processing operation, they are entitled to receive compensation from the Member State responsible for the damage suffered. Each Member State must also provide for a national supervisory authority, established in accordance with Directive 95/46/EC, to monitor the lawfulness of the processing of personal data. However, since the VIS database is based on a central platform and different national interfaces, and in the future will be interlinked with other databases on a European level, a real European supervision becomes essential. At the moment, the European Data Protection Supervisor only monitors the activities of the Commission in this regard.

3.2.3 Eurodac

The legislative framework of Eurodac is founded on 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[77].

The Decision has since been amended by:

- Council Regulation 407/2002/EC of 28 February 2002 laying down certain rules to implement Regulation 2725/2000/EC concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention[78]
- Council Decision 2006/188/EC of 21 February 2006 on the conclusion of the Agreement between the European Community and the Kingdom of Denmark extending to Denmark the provisions of Council Regulation 343/2003/EC establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and Council Regulation 2725/2000/EC concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention[79]..
- Council Decision 2008/147/EC of 28 January 2008 on the conclusion on behalf of the European Community of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland[80].

Discussion on other agreements and protocols on the participation of and cooperation with third countries are ongoing. At the moment there is also a legislative proposal on the use of Eurodac by national law enforcement authorities and by Europol[81].

The stated goal of the Eurodac system (which stands for European Dactyloscopie) is to enable Member States to identify asylum applicants and persons who have been

---

77 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:316:0001:0010:EN:PDF>

78 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:062:0001:0005:EN:PDF>

79 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:066:0037:0037:EN:PDF>

80 Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:053:0003:0004:EN:PDF>

81 See EDPS opinion of 7 October 2009 on this proposal at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-10-07_Access_Eurodac_EN.pdf>

apprehended while unlawfully crossing an external frontier of the Community. By comparing fingerprints, Member States can determine whether an asylum applicant or a foreign national found illegally present within a Member State has previously claimed asylum in another Member State or whether an asylum applicant entered the Union territory unlawfully. The national authorities that have access to the central database for the above-mentioned purpose are designated by the Member States itself.

In addition to the fingerprints, data sent by Member States include in particular the Member State of origin, the place and date of the asylum application if applicable, sex, reference number, the date on which the fingerprints were taken and the date on which the data were forwarded to the Central Unit. Data are collected for anyone over 14 years of age and are entered directly into the database by the Central Unit.

In the case of asylum applicants, data are kept for ten years unless the individual obtains the citizenship of one of the Member States, in which case their particulars must be immediately erased. Data relating to foreign nationals apprehended when attempting to cross an external border unlawfully 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, if the foreign national has left the territory of the Member States, or if the foreign national has obtained citizenship of a Member State.

Eurodac consists of a Central Unit within the Commission (the proposal for a Regulation of 3 December 2008 wants to assign this competence to a 'Management Authority' within the EU) equipped with a computerised central database for comparing the fingerprints of asylum applicants and a system for electronic data transmission between Member States and the database (i.e. the Automated Fingerprint Identification System - AFIS). The Central Unit defines the technical requirements for transmitting fingerprints electronically. A reference number makes it possible to relate a fingerprint to one particular person and to identify the Member State that sent the data. Member States must ensure the transmission of fingerprints in 'an appropriate quality' for the purpose of comparison. 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, they are not stored by Eurodac. The proposal for a Regulation of 3 December 2008 also advocates the interoperability of Eurodac with other large IT-systems, such as VIS and SIS II which would give a whole new dimension to an already privacy-invasive tool.

As regards the protection of personal data, Member States of origin must ensure that the taking of fingerprints and all operations involving the use, transmission, conservation or erasure of the data themselves are carried out lawfully. The Commission must see to the proper application of the Regulation within the Central Unit, and take the necessary measures to ensure the security 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. In addition to the national supervisory bodies, the European Data Protection Supervisor

(EDPS), an independent supervisory body, has to ensure that the rights of data subjects affected by Eurodac are protected.

The Regulation applies to the territories to which the Dublin Regulation applies, namely all Member States, Iceland, Norway and the Swiss Confederation. The Regulation is operable since 15 January 2003.

3.2.4 Eurosur

The concerned legislation is the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Examining the creation of a European border surveillance system (EUROSUR)[82].

The stated goal of a "European border surveillance system" (EUROSUR) is to support the Member States in their efforts to reduce the number of illegal immigrants entering the European Union undetected, to reduce the number of deaths of illegal immigrants by saving more lives at sea, and to increase the internal security of the EU as a whole. To this end, a common technical framework will be created that contributes to the situational awareness at the external borders of the EU and increases the reaction capability of the information, border control and law enforcement authorities. One essential operational objective must be to create an information-sharing environment among national and European systems. While the Communication does not give details on the personal data to be collected and processed in the framework of Eurosur, it simply mentions that these processing should observe the general EU principles on the protection of personal data, consequently appropriate legislative measures defining the nature of the processing and laying down appropriate safeguards will need to be developed.

Eurosur will be implemented in three phases. The first phase aims at interconnecting, rationalizing, modernizing and expanding border surveillance systems at national level and creating national external border control coordination centers in the Member States. A secured computerized communication network will be set up to exchange data and facilitate the coordination of activities between national centers and Frontex. Consideration will also be given to means of providing financial and logistical assistance to certain neighboring third countries to promote operational cooperation with the Member States in border surveillance.

The second phase aims at improving the performance of surveillance tools at EU level. The shared application of surveillance tools could provide Member States' authorities with more frequent and more reliable surveillance information on their external borders and pre-frontier area. Finally, a common pre-frontier intelligence picture could be established, combining the information provided by intelligence services and surveillance tools.

The third phase aims at creating a common monitoring and information-sharing environment for the EU maritime domain. The objective here would be to integrate into a broader network all existing sectoral systems reporting and monitoring traffic and activities in sea areas under the jurisdiction of the Member States and in adjacent high seas, thus allowing border control authorities to take advantage of the integrated

[82] Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0068:FIN:EN:PDF>

use of these various systems. Ultimately, this integrated network of reporting and surveillance systems could be expanded to the EU's entire maritime domain, going beyond border-related aspects to cover all maritime activities, including maritime safety, protection of the marine environment, fisheries control and law enforcement.

Phases 1 and 2 will be limited to external land and sea borders, while phase 3 will focus exclusively on the maritime domain. The aspects of this Communication dealing with surveillance of external maritime borders form part of the overall framework set by the Integrated Maritime Policy for the European Union. Once implemented, EUROSUR would constitute a decisive step in the further gradual establishment of a common European integrated border management system which is intended to make border checks as 'efficient' as possible, integrating all checks and controls for different purposes. However, it is another example of how European governments and EU policy-makers are pursuing unfettered powers to access and gather masses of personal data on the everyday life of people on the grounds that we will be more safe and secure from perceived 'threats'.

4 Main recommendations on emerging technologies

4.1 RFID

A new hot topic on the European Commission issues has been since 2006 the Radio Frequency Identification (RFID) technology. This new technology allows the automatic identification of objects by a smart tag that can be read by RFID readers.

Starting with 2006, a yearly EU Roadmap on RFID was produced by the European Commission[83], trying to identify the major problems and regulatory solutions that could appear in relationship with this new technology. After a public consultation in 2007, the answers highlighted that the major problems are related with the privacy issues of using RFID technology[84], as it is able to process personal data collected from different sources.

The main problems related to privacy have been highlighted by EDRi in several[85] public documents presented also in the RFID Expert Group Meetings. Thus by establishing a a global identification system for objects it will lead to a global system identifying persons that are related to objects. The RFID applications need to have a built-in system of „security and privacy-by-design", in order to respect the data protection principles, otherwise the usage of the RFID chips will have the possibility to track consumers without their consent.

---

[83] See <http://www.iot-visitthefuture.eu/fileadmin/Timeline/2006/EU_RFID_Roadmap_2006/2006_EU_RFID_Roadmap.pdf>

[84] See <http://www.iot-visitthefuture.eu/fileadmin/Timeline/2007/Communication_2007/150307_Results_Public_Online_Consultation_on_RFID_Policy_Brussels.pdf>

[85] See <http://www.edri.org/docs/EDRi_RFID_Privacy_Issues_published.pdf , http://www.edri.org/docs/EDRi_RFID_Informed_Consent_published.pdf>, and <http://www.edri.org/docs/EDRi_RFID_Security_Issues.pdf>

The privacy concerns are related with the possibility to infer a person's behaviour by monitoring a specific group of RFID tags, to associate the person with a specific RFID tag, that can also identify the location of that person. Through communication between RFID readers, it is possible to track people, based on items that contain RFID tags that are being carried. Also the right to delete the personal data is unclear how it works in an unregulated RFID system, especially if the connections between a person and an item identified by an RFID tag are irrevocably deleted or the connection could be reconstructed at a specific time even after the deletion.

Other privacy concerns are related with the security of these devices, starting with the possibility if cloning then and ending with the decision on who is allowed to collect data on tagged objects is taken by the person or organisation that mounts the tag on the object. In most of today's RFID Systems the data on the tag is accessible by anyone who is able to operate a RFID reader.

The European Data Protection Supervisor, in his opinion[86] on the 2007 Communication from the European Commission ((2008/C 101/01) identified 5 basic privacy and security issues for RFID systems:

- identification of data subject
- identification of the controller
- the decreased meaning of the traditional distinction between the personal and the public sphere
- the size and the physical properties of RFID-tags
- lack of transparency of the processing.

After several months for public consultation on the matter, the European Commission published in 2009 a Recommendation and a Communication on the RFID issues.

The Commission Recommendation of 12 May 2009 on the use of RFID was issued in 12 May 2009[87] and was asking retailers using RFID tags to store and track products to deactivate them at the point of sale thus avoiding potential privacy and security problems. The opt-in principle was included in the recommendation, giving customers the possibility to agree to keep their tags active if they wish to. Tags are to be deactivated should customers fail to opt-in.

The Commission also recommends organisations using RFID systems to assess the possible impact on privacy and data protection before using them, to act in order to minimise "any risk of infringing people's rights", to inform people who may be affected that the systems are in use by means of an established logo that can be defined by standardisation organisations and to inform the operators of the RFID systems on their purpose. According to the recommendation, the national authorities should do their best to increase the awareness of the public and small businesses on

[86] Available at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf>

[87] See <http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf>

the matter and to encourage research and development for more secure and privacy friendly RFID systems. Retailers are expected to use an established logo indicating the use of a RFID tag on a product, to deactivate and remove such a tag in case of risks to customers' privacy or personal data security and even offer to do so even if there is no such risk.

According with the text on the 2009 Recommendation, until 2011 the member States are to inform the Commission on the measures they intend to take in order to meet the objectives of the Recommendation and within two-three years, the Commission will report on the Recommendation's implementation including an impact analysis on citizens as well as companies and public authorities using smart chips.

A second important document in current EU RFID Policy was issued by the European Commission on the 18 June 2009 called Internet of Things — An action plan for Europe[88] This communication from the European Commission (COM(2009) 278 final) included a 14-point action plan to address the main issues raised from the RFID usage as discussed in the working group and in the consultation period. One of the most important action point was the launch of "a debate on the technical and legal aspects of the 'right to silence of the chips', which has been referred to under different names by different authors and expresses the idea that individuals should be able to disconnect from their networked environment at any time." The communication underlined that these rights will have an influence on how the Internet of Things is conceived but, at the same time, its development will affect the way we understand privacy.

The communication points on the policy that this new field can be left for self-regulation, but rather it would need to discuss the concept of governance of the RFID usage in order to establish a set of principles and to set up an "architecture" with a sufficient level of decentralised management.

4.2 CCTV

The concerned legislation is 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 (OJ L 281, 23/11/95) and the applicable national legislation.

The e-Privacy Directive does not apply to the CCTV (Closed-circuit television) services since they are not included in the definition of electronic communication services.

The principles of data protection, as express by Directive 95/46/EC do apply on CCTV services, if the owners of these services are data controllers established in one of the European Union member states. This applies to the CCTV's processing of personal data, including image and sound data, irrespectively if they are made entirely or just partly automatic.

The privacy concerns of the CCTV are not related not only with processing of personal data, without a proper information of the data subject, but also with the necessity and proportionality of this measure. As more European Union countries use

[88] Available at <http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf>

CCTV in more instances for every day life, they usually lack a proper justification or enough evidence that this is indeed useful. Although some of the European countries have adopted secondary legislation, based on the EU Data Protection directive, their enforcement are varying a lot from country to country.

New technological developments are also raising future privacy issues, especially with the deployment of Computerised Face Recognition systems that may automatically compare and recognise faces from a database of facial images, micro and miniature video recording devices that allow covert surveillance and technology that allows video images to be taken in darkness or detecting motion behind walls.

The Article 29 Working Party has issued in 2004 an Opinion on the Processing of Personal Data by means of Video Surveillance[89], which highlights the main problems in interpreting the EU Data Protection Directive in relation with the video surveillance practices:

- The lawfulness of the video surveillance practice – especially in relationship with general public security purpose and other purposes;
- The clear specifications of the purposes and their lawfulness, as explained in the notification to the competent Data Protection Authority;
- The criteria that makes the data processing legitimate;
- The proportionality of the measure to start using CCTV, especially by considering if other mechanism are clearly insufficient or inapplicable;
- The proportionality in implementing the activities of video surveillance activities, including the decision on retention of the images and video and for what period;
- The implementation of the principle of providing adequate information to data subjects
- The security measures that are implemented in agreement with the minimum standards in this field, as express by the national Data Protection Authority;
- The specific implementation of the rights of the data subjects;
- The additional safeguards in connection with specific processing operations (such as association with other biometric data, usage of voice identification systems, use of facial recognition systems of automated decision).

The Article 29 Working Party has also issued opinions that include information on how the data protection legislation applies to video surveillance techniques in two specific contexts, that may create additional privacy concerns. The first one is related to the video surveillance in employment. (Opinion no. 8/2001 on the Processing of Personal Data in the Employment Context and Working Document on the Surveillance of Electronic Communications in the Workplace[90]), where the Working

[89] Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf>

[90] Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf>

Party agrees that „video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities, therefore entailing the processing of personal data in this context, should not be permitted as a rule."

The second one is related to the use of CCTVs in Schools (Working Document 1/2008 on the protection of children's personal data - (General guidelines and the special case of schools))[91]. Although the document underlines that it can't suggest an overall solution for all cases, it also highlights the necessity of a prior "thorough discussion between teachers, parents and pupils' representatives, taking into account the stated aims of the installation and the adequacy of the proposed systems."

The European Data Protection Supervisor has been also been active in this field by checking the implementation of the CCTVs in various EU institutions to see if they fulfil the data protection principles (such as Opinion on the notification for prior checking received from the Data Protection Officer ("DPO") of the European Anti-Fraud Office ("OLAF") on 17 October 2007 regarding OLAF's CCTV system[92]) The EDPS is also planning to issue in 2010 guidelines to European institutions and bodies using video-surveillance in agreement with the data protection rules.

At the same time, the European Union is also spending a lot of efforts in promoting the video surveillance as a useful tool for enhancing security, including by the adoption of the 2006 Green Paper on detection technologies in the work of law enforcement, customs and other security authorities[93].

4.3 Social networks

Online Social Networks or Social Networking Sites (SNS) are one of the most remarkable technological phenomena of the 21st century, with several SNSs now among the most visisted websites globally. SNSs may be seen as informal but all-embracing identity management tools, defining access to user-created content via social relationships.

The commercial success of the multi-billion euro SNS industry depends heavily on the number of users it attracts. Combined with the strong human desire to connect, this encourages design and online behaviour where security and privacy are not always the first priority. Users are often not aware of the size of the audience accessing their content. The sense of intimacy created by being among digital 'friends' often leads to inappropriate or damaging disclosures. SNS members for example broadcast information much more widely and sometimes unadvisedly, either by choice or unwittingly.

---

91 Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf>

92 Available at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2008/08-05-19_OLAF_CCTV_EN.pdf>

93 Available at <http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0474en01.pdf>

There are several threats[94] concerning SNS, of which the most important are the following. First of all, there is the risk of aggregation of digital dossiers. Profiles on online SNSs can be downloaded and stored by third parties, creating a digital dossier of personal data. There is the risk of secondary data collection: next to data knowingly disclosed in a profile, SN members disclose personal information using the network itself (e.g. length of connections, other users' profiles visited and messages sent). SNSs provide a central repository accessible to a single provider. The high value of SNSs suggests that such data is being used to considerable financial gain. There is also the risk of face recognition, since user-provided digital images are a very popular part of profiles on SNSs. The photograph is, in effect, a binary identifier for the user, enabling linking across profiles. There is the risk of content-based image retrieval (CBIR), which is an emerging technology that can match features, such as identifying aspects of a room (e.g. a painting) in very large databases, increasing the possibilities for locating users. There is the risk of linkability from image metadata. Many SNSs now allow users to tag images with metadata, such as links to SNS profiles (even if they are not the owner/controller of that profile), or even e-mail addresses. This leads to greater possibilities for unwanted linkage to personal data. Of course, there is also the difficulty of complete account deletion. Users wishing to delete accounts from SNSs find that it is almost impossible to remove secondary information linked to their profile such as public comments on other profiles.

Other, less common, SNS threats include spear phishing using SNSs. These are highly targeted phishing attacks, facilitated by the self-created 'profiles' easily accessible on SNSs. SNSs are also vulnerable to social engineering techniques which exploit low entry thresholds to trust networks and to scripting attacks which allow the automated injection of phishing links. Next to this, there is the risk of infiltration of networks. Some information is only available to a restricted group or network of friends, which should provide the first line of defence in protecting privacy on SNSs. However, since it is often easy to become someone's 'friend' under false pretences, this mechanism is not effective. On many SNSs it is even possible to use scripts to invite friends. There is also the risk of profile-squatting and reputation damage through ID theft, whereby fake profiles are created in the name of well-known personalities or brands or within a particular network (such as a school class) in order to slander people or profit from their reputation. There is the risk of stalking. Cyberstalking is threatening behaviour in which a perpetrator repeatedly contacts a victim by electronic means such as e-mail, Instant Messenger and messaging on SNSs. Statistics suggest that stalking using SNSs is increasing. Finally, there is the risk of cyber-bullying. SNSs can offer an array of tools which facilitate cyberbullying, i.e. repeated and purposeful acts of harm such as harassment, humiliation and secret sharing.

In conclusion, SNSs present several scenarios which were not foreseen when current legislation, especially data protection law, was created. This means that certain issues may need to be clarified and, in some cases, the existing legal framework may even need to be modified or extended. Specific issues include for example the legal position on deletion of user-generated content by service providers if it is classed as SNS spam; the legal position on image-tagging by third parties; the legal position on profile-squatting; designating who is responsible for security flaws resulting from user-generated markup or scripting; designating how privacy policies of embedded

[94] After: HOGBEN, G., ENISA Position Paper No.1 "Security Issues and Recommendations for Online Social Networks", October 2007, 33p.

third party widgets should be communicated to users; defining what exactly constitutes personal data in an SNS environment and how to increase transparency of datahandling practices; and finally, decide whether the posting of certain classes of data by minors (location data) should be made illegal.

While efforts have started at EU level to address the personal data protection issue in SNS, they are still limited, mainly because major SNS providers are non EU companies. Most of them are still based on seld-regulation means, such as agreements of charters and principles.

On 17 February 2009, some 20 leading European and non European web firms signed the "Safer Social Networking Principles for the EU"[95], during the Safer Internet Day in Luxembourg. These principles have been developed by SNS providers in consultation with the European Commission, as part of its Safer Internet Plus Programme, and some NGOs dealing with child protection, in order to provide good practice recommendations to enhance the safety of children and young people using SNS. The principles mainly concern children protection against illegal content and conduct, and show limited interest on the protection of privacy and personal data. In particular, these principles do not address the collection and processing of personal data by SNS providers, nor do they address the retention period of these data.

On 12 June 2009, the Article 29 Data Protection Working Party adopted an opinion on online social networking[96]. In addition to advocating robust security and privacy-friendly default settings, this Opinion brings important legal clarifications. It asserts the applicability of European law on data protection to SNS, even if their headquarters are located outside Europe; it states that SNS providers and, in many cases, third party application providers, are data controllers; and it specifies that SNS fall outside the scope of the definition of electronic communication services. Therefore, the Opinion clarifies the fact that on the one hand SNS indeed falls under the 95/46/EC Data Protection Directive and on the other hand, regarding the data retention period, the 2006/24/EC Data Retention Directive does not apply, except for specific additional services like e.g. publicly accessible email services, thus the claim that personal data of SNS users need to be retained up to 24 months by SNS providers is not valid.

4.4 Search engines

The concerned legislation is 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 and the applicable national legislation. Search engine services in the strict sense do not in general fall under the scope of the new regulatory framework for electronic communications of which the e-Privacy Directive is part. Also, the Data Retention Directive 2006/24/EC

---

[95] Available at <http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf>

[96] Available at <http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_25_06_09_en.pdf>

is clearly highlighted as not applicable to search engine providers since this Directive prohibits explicitly the retention of data revealing content such as search queries.

Directive 95/46/EC applies to search engine providers as controllers of user data and as providers of contact data, even when their headquarters are located outside the European Union. In the case of a search engine service provider that is established in, and provides all of its services from one or more, Member States, data protection rules are not restricted to data subjects on the territory or of a nationality of one of the Member States. Where the search engine service provider is a non EU-based controller, there are two cases in which Community data protection law still applies. Firstly, where the search engine provider has an establishment in a Member State, and secondly, where the search engine makes use of equipment on the territory of a Member State. In the latter case the search engine has to designate a representative in the territory of that particular Member State.

The Article 29 Data Protection Working Party has published a detailed Opinion on 4 April 2008[97], analyzing the applicability of EC Directives to search engines and clarifying the obligations of search engine providers.

In their role as service providers to users, search engines collect and process vast amounts of user data**,** including data gathered by technical means, such as cookies. Data collected can range from the IP address of individual users to extensive histories of past searching behaviour or data provided by users themselves when signing up to use personalised services. It is the opinion of the article 29 Working Party that search engines in their role as collectors of user data have so far insufficiently explained the nature and purpose of their operations to the users of their services.

Second, in their role as content providers, search engines help to make publications on the internet easily accessible to a worldwide audience. Some search engines republish data in a so-called 'cache'. By retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate. The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive. Any kind of personal information posted on a website could be used by a third party for profiling.

Search engines may only process personal data for legitimate purposes and the amount of data has to be relevant and not excessive in respect of the various purposes to be achieved. Search engine providers must delete or anonymise (in an irreversible and efficient way) personal data once they are no longer necessary for the purpose for which they were collected. Retention periods should be minimised and be proportionate to each purpose put forward by search engine providers. According to the Article 29 Working Party, this should be limited to 6 months. However, national legislation may require earlier deletion of personal data. In case search engine providers retain personal data longer than 6 months, they must demonstrate comprehensively that it is strictly necessary for the service. In any case, the

[97] Available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf>

information about the data retention period chosen by search engine providers should be easily accessible from their homepage.

While search engine providers inevitably collect some personal data about the users of their services, such as their IP address, the Article 29 Working Party finds it necessary to collect additional personal data from individual users in order to be able to perform the service of delivering search results and advertisements. If search engine providers use cookies, their lifetime should be no longer than demonstrably necessary. Similarly to web cookies, flash cookies should only be installed if transparent information is provided about the purpose for which they are installed and how to access, edit and delete this information. Search engine providers must give users clear and intelligible information about their identity and location and about the data they intend to collect, store or transmit, as well as the purpose for which they are collected.

Enrichment of user profiles with data not provided by the users themselves is to be based on the consent of the users. If search engine providers provide means to retain the individual search history, they should make sure they have the consent of the user. Search engines should respect website editor opt-outs indicating that the website should not be crawled and indexed or included in the search engines' caches. When search engine providers provide a cache, in which personal data are being made available for longer than the original publication, they must respect the right of data subjects to have excessive and inaccurate data removed from their cache. Search engine providers that specialise in the creation of value added operations, such as profiles of natural persons (so called 'people search engines') and facial recognition software on images, must have a legitimate ground for processing, such as consent, and meet all other requirements of Directive 95/46/EC, such as the obligation to guarantee the quality of data and fairness of processing.

Users of search engine services have the right to access, inspect and correct if necessary, according to Article 12 of Directive 95/46/EC, all their personal data, including their profiles and search history. Cross-correlation of data originating from different services belonging to the search engine provider may only be performed if the user for that specific service has granted consent. However, this touches the issue of 'informed' consent.

This Article 29 Opinion of 2008 included a questionnaire for search engines on their privacy policy, and served as a basis point for numerous meetings and letters exchanges with main EU and non EU search engines providers, in order to address the three major topics of data retention period, anonymisation, and applicable laws[98].

5 Conclusion

As already set in the introduction of this report, this document is meant as providing a comprehensive description and assessment of the European Union situation with respect to privacy and personal data protection as of August 2009. The authors hope the documents will serve as a tool to better understand the European legislation and regulation in this matter, as a good basis for further updates and, last but not least, as a

[98] See related press releases and other documents from the Article 29 working party at <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/>

useful vehicle for better participation in European and national political debates on privacy and data protection.

One of the main issues in such debates is the issue of control. Reaffirming principles such as the proportionality and limited purpose is not enough. The EU legislation must implement actual guarantees, which are not currently adequately fulfilled.

Among the main observed trends are the extension of purposes, the enlargement of scope and means of the databases, and the fact that they more and more target vulnerable groups, such as migrants, minorities, children and youngster. Minor are particularly targeted in many EU countries, where children can have their DNA taken and filed in national DNA database and where intelligence databases looking to prevent public security infractions may register children. In some countries, databases once set up to fight terrorism and serious crime are now used to fight minor delinquency.

Current protecting legislation does not provide enough guarantees. The EU Data Protection Framework Decision, which rules data protection under 3rd pillar (police and justice cooperation), has only been adopted in December 2008. Yet, it still lacks protection with regards to the transfer of member States domestic data to third countries, which means that, for instance, it does not apply to the transfer of European airline passenger data (PNR) to the USA.

Moreover, these databases lack protection against loss or theft of data. The revision of the EU Telecom package included some provisions on data breach notification, but they are mandatory only for Internet service providers and telecom operators.

Biometric identity (as in passports and national identity cards) is an important issue in Europe, with the creation in many countries of national centralized databases containing biometric identifiers. The biometric passport, which is an obligation since the 2004 Regulation of the EU Council, has been an opportunity for some member States to go beyond EU requirements.

Despite important resistances at national level in many countries, the data retention Directive of 2006 has been implemented, sometimes going beyond the Directive requirements in terms of retained categories of data. This Directive needs to be revised so as to end its data retention requirements.

These are only some of the main concerns currently at the EU level, and the need is growing for better data protection provisions at EU level, such as:

- The need to establish actual implementation of the proportionality and purpose limitation principles;
- The need to drastically limit the use of biometric and genetic data;
- The need to better protect against risks of uncontrolled data sharing; and
- The need to better protect of vulnerable groups.